SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report

1987-1988

89-05714/

Security Intelligence Review Committee
14th Floor
365 Laurier Avenue West
P.O. Box 2430, Station D
Ottawa, Ontario
K1P 5W5

(613) 990-8441: Collect calls are accepted, and the switchboard is open from 7:30 a.m. to 6 p.m. Ottawa time.

© Minister of Supply and Services Canada 1988

Cat. No. JS 71-1/1988

ISBN 0-662-56247-X

September 30, 1988

The Honourable James F. Kelleher, P.C., M.P., Q.C.
Solicitor General of Canada
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Kelleher:

Pursuant to section 53 of the *Canadian Security Intelligence Act*, we hereby transmit to you the Annual Report of the Security Intelligence Review Committee for the fiscal year 1987-88, for submission to Parliament.

Yours sincerely,

Ronald G. Atkey, P.C., Q.C.
Chairman

Jean Jacques Blais, P.C., Q.C.

Frank McGee, P.C.

Saul M. Cherniack, P.C., Q.C.

Paule Gauthier, P.C.

Turning the corner

Contents

1. **A Second Wind** 1

Good Calls and Bum Raps 1
Our Responsibility 2
Business Not as Usual 3

2. **Oversight** 5

Warrants 5
Ministerial Instructions 5
Agreements with Other Organizations 6
Disclosures in the Public Interest 7
Unlawful Acts 7
CSIS Annual Report and Certificate of the Inspector General 8
Statistics on Operational Activities 8
Special Studies 8
Budgeting Information 9
Consultations 10
Inquiries and Briefings 10
Our Relations with CSIS 11

3. **CSIS Operations** 13

Counter-subversion Operations 13
Fall-out 1: Files 14
Fall-out 2: Targeting and Warrants 14
A Case in Point 16
Open Sources 17
Warrant Statistics 18
Security Screening 19

4. **Inside CSIS** 21

The Academy Revisited 21
Representation and Bilingualism 21
Polygraph Testing: From Bad to What? 23
Management 24

5. **Counter-terrorism Operations** 27

CSIS's Mandate 27
Our Study: Issues and Methods 27
The Challenge 28
Increased Priority 29
Targeting and Investigations 29
Policies and Practices 31
Intelligence Production 32
Conclusion 33

6. **From Information to Intelligence** 35

The Intelligence Product 35

Setting Priorities 36
Sources and Methods 37
Specialization 38
Meeting User Needs 39
Options for the Future 40
Summing Up 41

7. Complaints 43

The 1987-88 Cases 43
Who Decides? 44
Disclosure 45

8. Inside SIRC 47

Our Work as Members of SIRC 47
Financial Report 47
Personnel 48

9. Need to Know 49

Intelligence Directory 49
Reaching Out 49
Canadian Scholarship 50
Media: Friend, Foe . . . or Both? 51
Speaking Up for CSIS 51

10. Five Years Later 53

Security Intelligence and Public Policy 53
Security Intelligence and the Wider Community 54
The Dissemination of Intelligence 54
Threats to the Security of Canada 55
Security Clearances 56
CSIS Operations 57
Controls on Warrants 57
Oversight 58
Access to Information and Privacy 59
Basically Sound 59

Appendices

A Ministerial Instructions 61
B Case Histories 63
C The Intelligence Network in Canada 67
D SIRC Staff on July 1, 1988 77

1. A Second Wind

We hope our successors will be able to look back and say that 1987-88 was the year the Canadian Security Intelligence Service (CSIS) turned the corner.

It was a year in which CSIS faced perhaps its darkest moments, capped by the resignation of its first Director after the Atwal warrant affair (see page 11). With the requirement for secrecy that is central to its operations, CSIS cannot have been pleased about the number of "outsiders" who came through its doors. First there was the Independent Advisory Team, armed with the conclusions of our last Annual Report and our special report on official languages and staff relations, *Closing the Gaps*, together with a mandate for change.* Then came a new Director appointed from outside the Service. The counter-subversion branch was disbanded and its duties reassigned. Even though operational work was not significantly affected, no one could blame the men and women of CSIS if they were sometimes frustrated.

But there is an up side to all of this. The Independent Advisory Team developed a realistic reform package on the basis of our recommendations, and the Government started to implement it. Disbandment of the counter-subversion branch will stem overreaction to the rather modest threats Canada faces from home-grown radicals. Early indications are that the new Director is providing active leadership.

In short, we feel that this difficult year brought CSIS the chance it needs to get a second wind and complete its evolution into the kind of agency that Parliament intended when it adopted the *CSIS Act* in 1984—a civilian agency with contemporary priorities, its attention focused on gathering and analysing security intelligence as a basis for solid advice to the government of the day.

Good Calls and Bum Raps

Some of the barrage of criticism CSIS faced last year was justified. Haste does not excuse the carelessness that allowed unreliable information to be used in obtaining Federal Court authority for the Atwal wiretap.

But nemesis was at work, and the Atwal affair brought its own punishment. Because of the flawed warrant, proceedings had to be suspended against five men accused of conspiracy to murder a minister of the state government of the Punjab in India. CSIS also came under public fire for failing to inform police in advance of the conspiracy. Conversations recorded in the wiretap pointed clearly to a plan to assault the minister, but CSIS did not review the material until the attempt had already been made.

---

* The Independent Advisory Team was appointed by the Solicitor General on July 22, 1987, and handed in its report, *People and Process in Transition*, with 34 recommendations, on October 28, 1987. Headed by Gordon Osbaldeston, a former clerk of the Privy Council and now a senior fellow at the School of Business Administration, University of Western Ontario, it also included Roger Tassé, a former deputy solicitor general and deputy minister of justice who now practices law privately, and Gérard Duclos, Deputy Controller General, Management Review Branch, Treasury Board.

This episode also contributed to an atmosphere of suspicion—not to say derision—in which all sorts of allegations about bungling and wrongdoing were floated. Looking into media reports and following up our own leads, we found that much of what was being said was mistaken. We found that:

- CSIS did *not* slip up in the entry into Canada of Mahmoud Mohammad Issa Mohammad; someone did, but it was not CSIS.
- *Nor* did it compromise his attempt to leave the country.
- There is *no* evidence to date that CSIS had usable and reliable information that might have prevented the Air India tragedy of June 23, 1985, when a jumbo jet bound from Toronto and Montreal to Bombay went down off the coast of Ireland at a cost of 329 lives; to have said that trouble was likely on an aircraft of Air India was good common sense but hardly a "tipoff" to a specific event.
- *Nor* was there any basis to conclude that there was a loss when wiretap tapes were routinely erased after the relevant information they provided had been noted.
- CSIS does *not* target the labour movement.
- It did *not* try to get the *Sûreté du Québec* to give one of its informers a break in the investigation of bombing incidents.
- Complaints to the media as well as to us by a man that he was being harassed were *not* founded; after investigation, we concluded that CSIS made reasonable inquiries in a reasonable way.

CSIS had its successes too. Unfortunately they are measured on an invisible scale—by what does not happen rather than by what does. But fair is fair. It is only fair to remember that 1987-88 was a year of unusually heavy demand for security intelligence as Canada welcomed the Francophone and Commonwealth summits in quick succession, then welcomed the world to the Calgary Olympics February 13-28. At year-end, CSIS and the police were cooperating to prepare for the Economic Summit in Toronto. It is a tribute to the dedication and professionalism of the men and women of CSIS at all levels that the year was without serious security incident.

We welcome the Solicitor General's initiative in launching a series of addresses describing CSIS's work and pointing up, in some detail, its importance to Canadians. Security considerations make it hard for CSIS to blow its own horn. Our perspective, by statute, is one of reasoned skepticism, so it is very appropriate for the Solicitor General to fill the public relations gap.

Our Responsibility

For our part, we believe that Parliament and the public expect the Security Intelligence Review Committee to have strong opinions and to state them clearly in its annual and special reports.

Our objective has been to be fair. Our special report on the so-called Boivin affair* makes the point. We found much that we did not like during the investigation we carried out after allegations were made that a union official, Marc-André Boivin, facing bomb-related charges was a CSIS informant, perhaps even an *agent provocateur*. We learned, for example, that CSIS had retained information originally gathered by the RCMP on trade unions and had not yet reviewed it in relation to the "strictly necessary" retention requirements of the *Act*. In our view, this was out of line with the *CSIS Act*. We were disturbed to find that the *Sûreté du Québec* was not alerted for two days after Mr. Boivin told his CSIS handler that specific and serious criminal offences might be imminent.

But we found that Mr. Boivin was not asked to, nor did he, report to CSIS on union affairs as such; his beat was "subversive" elements. Nor was there any evidence that CSIS ever directed or encouraged him to influence union business or to carry out illegal acts. He was not an *agent provocateur*. As far as targeting and tasking are concerned, CSIS was clean and we said so.

We intend to keep doing business as usual, advising Parliament and the public of the facts as we see them. That is the business Parliament gave us to do. Our hope is that the changes taking place in the way CSIS goes about its business will narrow our scope for criticism.

Business Not as Usual

As a matter of fact, the thread that ties together many of the problems we have flagged was a business-as-usual approach within the Service. We do not suggest an overt and conscious defiance of Parliament's decision in 1984 to change the approach to security intelligence. But CSIS often seemed to lack the will to adjust.

Perhaps that was unavoidable under the circumstances. It seems clear in retrospect that the dislocations of separation from the RCMP were underestimated—even at a material level: four years later, CSIS still does not have a proper headquarters of its own, for example; hundreds of CSIS officers still go to work every morning at RCMP headquarters on Alta Vista Drive in Ottawa.

In any case, during the first three years, the unquestioned need to keep security intelligence operations rolling was accepted by too many people at all levels as a reason—if not an excuse—to put off such matters as bringing files inherited from the RCMP into line with new statutory requirements, moving towards an acceptable level of official bilingualism, and aggressively searching out recruits with the research and policy backgrounds needed to do modern security intelligence work.

While 1987-88 has been a difficult time for CSIS, it has surely laid to rest any expectation that business can continue as usual. We have chosen the familiar expression "turning the

* *Section 54 Report to the Solicitor General of Canada on CSIS' Use of its Investigative Powers with Respect to the Labour Movement*, made public by the Solicitor General on March 29, 1988 (see Chapter 3 below for a fuller description of our findings and conclusions).

corner" for the epigraph of this year's Annual Report. Readers will find that we still have many criticisms, but we believe that CSIS is on the right road.

2. Oversight

Under the *CSIS Act*, the Security Intelligence Review Committee (SIRC) is Parliament's and the public's watchdog on the Service. Our mandate as a Committee is to see that CSIS carries out its work effectively, on the one hand, but without unreasonable or unnecessary intrusion on individual rights, on the other. Specific tasks assigned us by the *Act* fall into two broad categories—oversight and complaints. We also have a statutory obligation to report on our work once a year. In this, our Annual Report, we describe our work as fully as we can within the limits imposed by the need to protect national security.

Chapter 8 of this Report deals with the complaints process. In this chapter and the five that follow we report on our over ight activities under sections 38, 40 and 54 of the *Act*. Paragraph 38(*a*) directs us "to review generally the performance by the Service of its duties and functions" and lists a series of specific tasks. Paragraph 38(*b*) and section 40 provide for reviews aimed at "ensuring that the activities of the Service are carried out in accordance with this *Act*, [and] the regulations and directions issued by the Minister ... and that the[se] activities do not involve any unreasonable or unnecessary exercise by the Service of any of its powers". Under section 54, we may make special reports to the Solicitor General.

Because of its wide powers of investigation and the secrecy that unavoidably surrounds much of its work, CSIS comes under a number of controls. It can use its most intrusive powers—opening mail and tapping telephones, for example—only if it has warrants from the Federal Court of Canada. Each application for a warrant requires the personal approval of the Solicitor General. The Solicitor General has other controls as well. Formal agreements with provinces to ensure CSIS access to information held by police require his personal approval, and he issues formal instructions on the conduct of cases and entire classes of case. The Solicitor General has his own watchdog on CSIS, the Inspector General. Our oversight mandate extends to CSIS compliance with all of these controls.

Warrants

We expressed a number of concerns in last year's Annual Report about the targeting and warrant processes. As a result of the "mid-course correction" unveiled by the Solicitor General on November 30, 1987, CSIS has gone a very long way to meeting our concerns. The new arrangements are reviewed in Chapter 3 of this Report. The outstanding issues of solicitor-client privilege and emergency warrants, which may call for amendments to the *Act*, are dealt with in Chapter 10.

Ministerial Instructions

The 1987-88 ministerial directives we received are listed in Appendix A of this Report. After carefully examining 13 of them, we are of the opinion that they do not permit any unreasonable or unnecessary use of the Service's powers, nor do they impinge unduly on individual rights or privacy. In fact, most tend to circumscribe the independent authority of the Service and increase accountability to the Solicitor General. The same is true of two 1986-87 directives that arrived too late for us to review in our last Annual Report. Six 1987-88 directives arrived too late to be examined before this Report went to the press.

As promised (Annual Report 1986-87, page 6), we have begun to compile statistics on operations requiring ministerial approval. While security considerations prevent us from revealing the details of any operations, we can say they are very few in number.

In 1986-87 we discovered that we were not routinely getting copies of some documents we would consider ministerial directives or direction (Annual Report 1986-87, page 6) because of a narrow interpretation given to subsection 6(2) of the *CSIS Act*. The Department of the Solicitor General is in the process of developing criteria to ensure that we will be provided with everything properly falling under subsection 6(2). This process will be completed soon.

However, we discovered a new twist this year. In a news release dated February 25, 1988, the Solicitor General announced "new ministerial controls over CSIS investigations". (They provide that CSIS must have the Solicitor General's personal authority to conduct any intrusive investigation whatsoever in counter-subversion cases.) We found that these "new controls", while not the subject of formal written communications to CSIS by the Solicitor General, took the form of amendments to CSIS's Operational Manual.

The Manual is a compendium of step-by-step rules for CSIS employees. It is prepared by and is the responsibility of CSIS. It includes all ministerial instructions, of course. At many points it elaborates on these instructions in minute detail, prescribing forms to be used and lines of authority to be followed.

In accordance with subsection 7(1) of the *Act*, CSIS consults with the Deputy Solicitor General concerning general operational policies. In fact, the Deputy Solicitor General is consulted when the Manual is amended. We will henceforth give the same attention to changes in the Manual as to ministerial instructions under subsection 6(2) as they appear, in practice, to have equal standing.

Agreements with Other Organizations

Copies of nine new CSIS agreements with other organizations in Canada and one with a foreign agency were passed to us in 1987-88. We were satisfied with them as far as they went, but they raise two issues.

One is the completion of CSIS's arrangements with provinces for exchanges of information with police forces and for mutual assistance. Three of the nine domestic agreements signed last year are in this category. With the conclusion of an agreement with Manitoba soon after the end of the year under review, CSIS had agreements with all but one province—Quebec. The absence of a formal agreement does not by itself indicate a lack of cooperation that could compromise national security. But we are of the view that formal agreements are useful as an exercise in setting guidelines, so everyone knows what is permitted and, equally important, what is not.

The other issue is control over the transfer of personal information in the Service's hands. Most of the Service's agreements with departments and agencies of the federal government (which accounted, incidentally, for the other six domestic agreements we saw last year) cover the provision of information to CSIS under the terms of the *Privacy Act*. No exception can be taken to this.

But the CSIS management information system has not permitted easy identification of information and intelligence passed to other agencies. This effectively prevents us—short of making manual searches that would exhaust an army of researchers—from carrying out our statutory duty under subparagraph 38(*a*)(iii) of the *CSIS Act* to "monitor the provision of information and intelligence pursuant to those arrangements" with other agencies, both domestic and foreign.

We should say that the ongoing sampling we do has revealed no exchanges of information that we take exception to; information provided to others about residents of Canada was within the terms of the relevant agreements. Information exchanged under most of the relevant agreements is for visa vetting and security clearances.

However, we expect that a projected overhaul of the Service's computerized management information system will introduce programming that will permit easy access to data on information about Canadian residents exchanged by CSIS and other agencies (see Annual Report 1986-87, page 39). CSIS needs to be more attentive in general to keeping records of its activities, for the sake of its own monitoring as well as ours. And we wish to see a specific policy, guidelines and auditing procedure developed for the release of any information on a Canadian resident.

One bit of unfinished business (Annual Report 1986-87, page 18) was cleared away in 1987-88. CSIS prepared, at our request, a new descriptive catalogue of its arrangements with police and intelligence agencies in other countries. It was a considerable improvement over the incomplete list we were handed in 1985. After making inquiries about the nature of the agreements with 11 agencies in as many countries, we are satisfied that CSIS now has an up-to-date list of its international arrangements.

Disclosures in the Public Interest

Paragraph 19(2)(*d*) of the *Act* authorizes certain disclosures to public servants and to ministers other than the Solicitor General, the Secretary of State for External Affairs and the Minister of National Defence. Subsection 19(3) requires the Director to report such disclosures to us. None was reported in 1987-88.

In this connection, we have (Annual Report 1986-87, page 30) previously expressed concern that the *Act* makes no provision for warning individual Canadians when they are drawn into the orbit of front organizations that covertly serve purposes or foreign governments inimical to Canada's national security. If we do not expand on this theme here it is only because it is covered this year in Chapter 10, our look ahead to the five-year review of the *Act*.

Unlawful Acts

Two reports were given to us under section 20 of the *Act*. This section requires the Director of CSIS to advise the Solicitor General when it appears that an employee may have acted unlawfully in the course of duty. If the Solicitor General passes such a report on to the Attorney General of Canada, we get a copy together with any comments by the Solicitor General. In one case no charges were laid. In the second, the Attorney General

referred the matter to provincial authorities, which had not decided by year-end whether to lay charges. In both cases, we are satisfied that CSIS management is being strict in protecting the public from illegal acts that might be committed under the cloak of the *CSIS Act*.

CSIS Annual Report and Certificate of the Inspector General

Section 33 of the *CSIS Act* provides for an annual report to the Solicitor General by the Director of CSIS and for a certificate to be issued by the Inspector General saying whether the report is satisfactory—in particular whether the Service has done anything not authorized by the *Act*, anything in contravention of any instructions issued by the Solicitor General or anything that involves an unreasonable or unnecessary use by the Service of its powers. Section 33 further provides for the transmission of the Director's annual report and the Inspector General's certificate to us.

We are unable in this Report to comment on the 1987 certificate of the Inspector General, as there was no Inspector General at the time to issue one. Dr. Richard Gosse, who filled this office with distinction from its inauguration in 1984, left in February to become the first chairman of the Public Complaints Commission for the RCMP, and he had not been replaced by fiscal year-end. We take this occasion to thank Dr. Gosse for the cooperation he extended to us. We found that we could rely on his office to be thorough and industrious in the fact-finding it did on our behalf, as provided for in section 40 of the *Act*. He established a high mark for his successor to reach.

Statistics on Operational Activities

Subparagraph 38(*a*)(viii) of the *Act* gives us an explicit mandate "to compile and analyse statistics on the operational activities of the Service". We continue to compile and analyse statistics in a number of areas—the use of intrusive investigative techniques (e.g., the number of wiretaps authorized by warrants), the flow and retention of information (e.g., file retention; see page 14), and investigative levels (e.g., the number of field investigations in connection with security screening; see page 19).

CSIS meets with us at the drafting stage to discuss the eight to ten statistical papers we prepare each year. As a result, we reach our interpretations of the statistics in full knowledge of CSIS's interpretations, and these meetings are a useful learning experience for us.

Special Studies

We made two special reports to the Solicitor General under section 54 of the *Act* in 1987-88. One was on CSIS's use of its investigative powers with respect to the labour movement. As indicated in Chapter 1 above, it was made public by the Solicitor General on March 29, 1988. We discuss some of our findings in Chapter 3, below.

The other report was on security screening in immigration matters. The Solicitor General did not publish it because he believed that it contained sensitive national security information. But he noted in his response to us that it raised many important concerns, and it is

being used in an interdepartmental study prompted by recommendations made by the Standing Committee of the House of Commons on Labour, Employment and Immigration in its report of June 17, 1986.

Also, as we promised last year, we started a review of the system for safeguarding scientific and technological assets in Canada, relying primarily on structured interviews with federal officials involved in this area. We met with people from the Privy Council Office, Revenue Canada (Customs), the Department of External Affairs, the Department of National Defence, Supply and Services Canada and the RCMP, as well as with CSIS officials. Because of the large number of players in this field, the analysis and consultations leading to the final report are not yet completed.

We are pursuing a program of studies that will let us complete a comprehensive review of the basic functions of the Service by the time our mandate expires in 1989. In 1986-87 we reviewed the counter-subversion program, which raised serious questions about targeting—that is, the way CSIS selects subjects for investigation (see Chapter 3 of this Report for an update). This year we zeroed in on the counter-terrorism program (see Chapter 5) and intelligence assessment (Chapter 6). In the coming year, we will turn our attentions to the counter-intelligence program and CSIS investigations, if any, of the peace movement in Canada.

In carrying out these major studies, we have developed the practice of working out detailed terms of reference with the responsible CSIS managers. Thus they fully understand what information we need and can direct us to the appropriate files and documents. The Service, for its part, has developed the practice of designating a member from the unit under study to provide liaison. This officer works with us to manage the study in such a way that it interferes as little as possible with ongoing operational responsibilities.

Budgeting Information

We get the update of the Multi-year Operational Plan (MYOP) that CSIS, like all arms of the federal government, carries out annually. We recognize that the information in the Service's 1987 update meets Treasury Board's requirements. But it does not alone give us the bird's-eye view that we want to have of CSIS as an organization. It does not let us answer the question, does CSIS have the money and personnel it needs?

We should say that we have no evidence from the available information that CSIS is being spoiled by excess funding or staffing. If anything—and despite a sharply rising budget—we suspect that it is being asked to spread itself rather thin.

But we have now asked the Service for detailed corporate financial and human resources information. In particular, we have asked for a reconciliation of the MYOP data with data found in the Main Estimates, year-end audited financial statements such as those found for other agencies in the Public Accounts of Canada, and detailed information on the allocation of person years among various functions. We hope to complete a review of CSIS's resources and how it uses them before the end of our mandate.

Consultations

In our oversight role, we also have dozens of routine consultations. We meet the Solicitor General quarterly as a group, and our Chairman meets him monthly as well as occasionally meeting with the Deputy Solicitor General. The Chairman also meets regularly with the Director of CSIS. Both the full Committee and the Chairman meet occasionally with the Inspector General, and there are frequent meetings between the Inspector General and our Executive Secretary. In the past year, there were also meetings with the Independent Advisory Team created by the Solicitor General to follow up concerns we had expressed in past reports.

In 1987-88 we continued our practice of visiting regional and district offices of the Service rather than confining our contacts to Headquarters in Ottawa. This allows us to be briefed on regional operations by the people most in the know. We usually hold separate meetings with regional or district managers and with the rank and file so we can engage in frank exchanges in which we hear the concerns of people in the field and answer questions about our own role. CSIS has been very cooperative in this program. During the year under review we visited four regional and district offices—in Winnipeg, Vancouver, Montreal and Toronto. In the coming year, we will visit the Halifax and Quebec City offices as well as making return calls at Vancouver and Toronto.

Further afield, we made a tour of Hong Kong, Australia and New Zealand in November, 1987. In Hong Kong, we focused on the work done there to keep abreast of a flood of immigration requests. The number of immigration files originating in Hong Kong is about 25,000 a year and growing as people and money seek safe havens in anticipation of the takeover by China in 1997. What we learned there was of material help to us as we prepared our special report on security screening in immigration.

Australia and New Zealand are of particular interest as two countries with which Canada enjoys excellent relations. In addition, Australia's complaints process is close to ours—closer than that of any other country. What we learned there informs a number of our observations in this Annual Report.

Inquiries and Briefings

With the sole exception of cabinet confidences, we have access to all information in CSIS's hands. Last year we directed 95 written inquiries to the Service and had answers to 85 by year-end. That left a total of 10 questions unanswered at that time; of these, four were put to the Service in the last month of the fiscal year. As provided for in the *CSIS Act*, we sometimes have our fact-finding done by the office of the Inspector General. In 1987-88, the office of the Inspector General carried out three reviews of specific activities of the Service for us.

We also get briefings from CSIS on particular matters. Two that are of great public concern are the Air India disaster and the Narita Airport explosion, on which we received monthly updating in 1987-88. We have already, in Chapter 1 above, dealt with some allegations that have been made in the media. With regard to the erasure of tapes, it would be most improper for the Service to let wiretap tapes accumulate indefinitely in case they might eventually prove useful to the police. CSIS's job is to collect *intelligence*. Wiretap

tapes commonly include a great deal of personal and other information that does not belong in secret files. We believe CSIS is correct when it notes the pertinent information that its wiretaps provide, then destroys the tapes.

Beyond that, it is not for us to add to the public record on the Air India tragedy. We are deeply conscious of the frustration felt by Canadians that no charges have been laid three years later. The RCMP continues its investigation, and CSIS's role at the moment is to provide it with security intelligence assistance.* We will continue to monitor developments closely.

We also had briefings on the "Atwal warrant affair". The broad lines of this matter are on the public record as the result of proceedings in the Federal Court of Canada. What is perhaps not well understood is that the Service did not deliberately "cook" its warrant application by including information from a discredited source. When the affidavit was first drafted, the information was considered reliable. Only after the paperwork had moved to CSIS Headquarters did the regional office concerned decide that the source could not be trusted. The failure occurred when Headquarters was not notified. That is a serious matter, but it is not deliberate falsification. We believe that new procedures described in Chapter 3 improve the safeguards against lapses of this kind.

In another matter that came to public attention during the year, we satisfied ourselves that CSIS dealt properly with Ryszard Paszkowski, who went to the media in January, 1988, with a complex account of how his work for CSIS let him in for a year in a West German jail to complete a hijacking sentence. As the Solicitor General has confirmed in the House of Commons,** Paszkowski did work for CSIS after entering Canada illegally, but CSIS did not bring him into the country to be a double agent, as he claims, and it ended the relationship before Paszkowski voluntarily left Canada in August, 1986, and went to Italy, whence he was extradited by West Germany.

Our Relations with CSIS

Our relations with CSIS continue to be at arm's length. This is as it should be. We share an ultimate goal—effective security intelligence within the limits imposed by the values of a free and democratic society. But our roles are different and, to the extent we are both doing our job, they inevitably bring us into opposition at times.

In general, our reading is that CSIS plays by the book in dealing with us. In the oversight area, relations are at least correct. Often they are cordial. We have already noted in this chapter that CSIS has been very cooperative in arranging our visits to its regional offices and has put no obstacle in the way of our meetings with the rank and file separately from

* In the case of the Narita Airport explosion, legal proceedings are underway. The British police arrested a suspect in England on February 5, 1988. On August 9, 1988, the Magistrate in London ordered Inderjit Singh Reyat extradited to Canada to face charges, including two counts of manslaughter for the deaths at Narita. As this Report was going to press, the defendant had filed an appeal to that order.

** *Debates of the House of Commons*, January 22, 1988.

regional management. When we investigate specific complaints, relations are more distant and formal. That is also proper, because then we are acting in a quasi-judicial capacity.

We can well understand some wariness on the part of the Service; although we reject any suggestion that our exercise of review and investigative powers affects the Service adversely. Oversight in one form or another is becoming the common experience of Western intelligence agencies, but Australia is the only other country we know of where an independent body* has unrestricted access to security intelligence files.

We like to think of our relations with the Service in terms of creative tension. Although our reports are often critical of systems—the nature of our mandate ensures that they often will be—we want to express again our respect and admiration for the people who work for the Service. They have a difficult role in which, as it has often been observed, the successes must remain secret while the inevitable failures always seem to become known.

* The Inspector General.

3. CSIS Operations

The essence of CSIS's mandate is spelled out in section 12 of the *CSIS Act*. It says that CSIS "shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada".

"Threats to the security of Canada" are defined in section 2. They fall into four categories—espionage or sabotage, foreign interference in Canadian affairs, the use of violence to gain political ends in Canada or another country and, fourth, covert or potentially violent attempts to overthrow our constitutionally established system of government. "Lawful advocacy, protest or dissent" are explicitly excluded unless they are carried on in conjunction with any of the threats spelled out in section 2.

In Chapter 2 we dealt with controls on the Service's use of its powers in carrying out its mandate. This chapter and the three that follow review operational matters—how CSIS guards the security of Canada.

Counter-subversion Operations

In line with a recommendation in our last Annual Report (page 40), the counter-subversion arm of CSIS was disbanded in November, 1987, and its responsibilities were reassigned. As a result, CSIS investigation of home-grown threats to national security now better reflects their modest scale. It better reflects, too, the "strictly necessary" limit set out in section 12. Cases of suspected foreign activity inimical to Canada's interest are now handled by the Counter-intelligence Branch, while cases in which there appears to be a real risk of violence are handled by the Counter-terrorism Branch.

A residue of counter-subversion targets are now monitored by the Analysis and Production Branch, which adds to the files any relevant information that comes its way in the media or as a spin-off from other inquiries in order to provide the Government with what the Solicitor General has called "a watching brief".* But the Operational Manual has been amended so any active investigation of these cases in future will require the Solicitor General's personal authorization. We believe this is a good control; the initiative remains in CSIS's hands, sheltered from considerations of partisan political expediency, yet there is political accountability when an initiative is followed through.

In total, slightly more than 3,000 of the files that had been actively pursued in the counter-subversion program remain open. But only a small percentage of these are now under active investigation by the Counter-terrorism or Counter-intelligence Branches, the rest are only being monitored.

After examining targeting and the use of intrusive powers, we can affirm that from the time of the Solicitor General's announcement to year-end no group was subject to investigation solely under paragraph 2(*d*) of the *Act*—the "counter-subversion" provision.

---

* Solicitor General of Canada, Notes for an Address to the Conference on Advocacy, Protest and Dissent, Queen's University, February 25, 1988.

Fall-out 1: Files

Controversy over the fate of the counter-subversion program brought to light much more factual information than had previously been available on the extent of the Service's stock of information on individual Canadians. In our last Annual Report (page 38), we said that the counter-subversion branch "probably [had] more than 30,000 files on individuals—how many more, no one knows". Now we do know, and our figure turns out to have been as conservative as we expected. The Service subsequently did the necessary research and turned up about 54,000 such files.

In the same passage, we said that only a small proportion of the people with counter-subversion files were under active investigation, but we did not reveal how many as this was classified information. CSIS subsequently told the media that the number was 3,867.

The vast majority of counter-subversion files already inactive a year ago have now been locked away pending review. These include all files on labour organizations. With the end of the moratorium on the destruction of files, many of these files should soon be on their way to the shredder, others to the closed collection of the Public Archives of Canada.

We also expressed concern in last year's Annual Report (pages 21-23) about material that CSIS inherited from the RCMP Security Service, including most of the counter-subversion files. We thought it likely that much of this material failed the "strictly necessary" test and did not relate to "threats to the security of Canada" as defined in section 2. In addition, we noted that because of the moratorium, tens of thousands of files that had outlived their usefulness were still on hand.

We do not quarrel with the moratorium as such. It was imposed in February, 1985, after the Deschênes Commission on war criminals found that some immigration files it needed had been routinely destroyed years before. In any case, now that it has been lifted a unit has been set up within CSIS to review files and designate those that are to be destroyed. Some 67,000 intelligence files slated for destruction by the RCMP, before the creation of CSIS, have already been destroyed. We will continue to monitor progress.

As to the retention in active files of information that was originally gathered by the RCMP and may not meet the tests of section 2 and section 12, CSIS has now started a review aimed at weeding out information that should not be there. We recognize that it will take years to go through all the files. We will also monitor progress in this exercise.

Furthermore, starting in January, 1988, no information can be placed on these files unless the subjects fall under new and tighter targeting procedures described below. In line with our recommendation (Annual Report 1986-87, page 38), detailed criteria that satisfy us have been developed for opening files on individuals and groups.

Fall-out 2: Targeting and Warrants

There has been action on a number of other issues we raised last year in the context of the counter-subversion study. CSIS has established a task force to review all policy and it is overhauling its Operational Manual to bring it into line with the *CSIS Act*.

With respect to warrants, change was hastened by the revelation last November that information from a discredited source had been left in a successful application before the Federal Court for authority to intercept telephone communications in a counter-terrorism investigation. Both CSIS and the Inspector General launched thorough reviews of warrants then in effect. In particular, the Service set about verifying and documenting every allegation of fact contained in warrant applications. We intend to review this exercise.

More important for the future, a number of measures were taken to improve accountability. Warrant coordinators ensure that all relevant policies and procedures have been respected when an application is made. All facts set out in the affidavits underwriting applications are documented. A new Affidavit Content Certificate places explicit responsibility on the four people who sign it. An analyst and unit head certify that the facts alleged are backed up by the CSIS data base. A chief attests to the reliability of the reports from which the facts were drawn and to the need for the powers requested. A director general certifies that the information required by subsection 21(2) of the *Act* has been provided.

Warrant applications now also include more discussion of the powers to be used. When a renewal is sought, the analyst reviews the information already obtained through the use of powers authorized by the warrant. If nothing useful was turned up, alternative investigative techniques must be considered.

The procedure for targeting has also been improved. Mirroring the warrant process, facts cited in any proposal to target an individual (a "Subject Evaluation Report" or SER) must be documented, and opinions and recommendations must be distinguished from the facts. A "complete and balanced description" of the proposed target's activities must be provided. We had urged (Annual Report 1986-87, page 38) that SERs "rely less on isolated incidents and more on coherent argument for the targeting decision that TARC [the Target Approval and Review Committee] is asked to make".

The consequences to national security if the powers concerned are not granted—in other words, the real need for the warrant—must also now be considered. The revised Operational Manual places a duty on investigators to ensure that the use of intrusive techniques is weighed against possible damage to constitutional rights and freedoms. As in the warrant process, when authorization of an investigation expires, an investigator seeking renewal must provide an Assessment Report, which turns the spotlight on whether there have been any changes in the initial assumptions—whether the target is still capable of carrying out its aims, for example.

There have been positive changes in the treatment of groups in accordance with recommendations made in our 1986-87 Annual Report. Investigation of people we have termed "second-stage targets"—those who come to CSIS's attention only because they are in contact with primary targets (Annual Report 1986-87, page 36)—is limited to identifying them.

Both TARC and the Warrant Review Committee now sit under the personal chairmanship of the Director, and the Warrant Review Committee includes a Justice Department lawyer to act as "devil's advocate", challenging the need for each warrant in the first place. In line with a recommendation we made in last year's Annual Report (page 38), a centralized index of all targets is maintained.

A remaining reservation is with the level at which the devil's advocate participates in the warrant application process. When we made this proposal in the first place (Annual Report 1986-87, page 9), we suggested that this official intervene before the Solicitor General or the Federal Court itself. We feel that the situation where the devil's advocate is a minority of one, outnumbered by other officials on the Warrant Review Committee, has not yet gone quite far enough. However, we understand that the proper role for the devil's advocate is currently under active consideration.

It remains to be seen how well the new procedures are respected in practice. But they certainly go a long way towards meeting many of the concerns we have expressed in the past (Annual Report 1986-87, pages 36-38). Early indications are encouraging. We have looked at some of the post-reform warrant applications, and we are initially satisfied with the change that has taken place. Compared with what we had seen before, they are models of precision, clarity and logic.

A Case in Point

The "Boivin affair" illustrates some of the concerns we have had—and some of the work CSIS had already done, before the recent flurry of changes, to bring its targeting practices into line with the *CSIS Act*.

This affair erupted when the media reported that Marc-André Boivin, an official of the Confederation of National Trade Unions (CNTU) facing bomb-related charges in the Quebec courts, was a CSIS source, perhaps an *agent provocateur* whose illegal activities were part of a CSIS plot to disrupt and discredit the labour movement. Using information gathered by the Inspector General, we looked into these allegations and the Solicitor General made our report public on March 29, 1988.*

We found that Mr. Boivin became a source for the RCMP in 1973 with instructions to monitor suspected criminal and "subversive" activities in the labour milieu. On two occasions he had brushes with the law in connection with his union work—in 1973 for causing a disturbance while picketing and in 1978 for putting glue in the locks of a public building. The RCMP told him in the 1978 incident that he was not to take initiatives "not in keeping with our policies and the law of the land". By 1983, the RCMP Security Service's labour desk was only monitoring, not investigating.

By the time CSIS took over from the Security Service in 1984, Mr. Boivin was no longer targeted on the labour movement. He was targeted on communists and foreign-influenced agents attempting to influence the labour movement. It is clear from documents and interviews that CSIS took pains to ensure that Mr. Boivin understood the limits on his assignment, that he had no mandate to report on union activities or on the activities of union members except as they directly related to communist or foreign influence.

Indeed, our investigation showed that CSIS has not directed any human source against any union or any individual union members in their union capacities. It also showed that

* *Section 54 Report to the Solicitor General of Canada on CSIS' use of its Investigative Powers with Respect to the Labour Movement.*

reports from sources knowledgeable about the labour movement did not include such matters as strike activities, international organization, membership, bargaining positions or general political, economic or social goals.

We were disturbed to learn that CSIS waited two days to inform the *Sûreté du Québec* after Mr. Boivin told it there would be bombing attempts in Drummondville and Montreal. But we found that Mr. Boivin had been given appropriate directions by the Service and that no improper attempts were made to protect him once the charges were laid.

We were also disturbed to find that CSIS still held files put together at a time in the 1970s, before the *CSIS Act*, when the RCMP did investigate unions as such. CSIS had added to these files in line with its normal procedures. Even in the absence of a targeting decision, CSIS researchers routinely posted any information that came their way in the appropriate file if there was one. We also found that these files were fully accessible to CSIS investigators.

The Solicitor General and the Director took action that we consider appropriate. Files on labour unions were locked up and are now awaiting review, and if they do not meet the criteria of the *Act* they will be destroyed or sent to National Archives. Instructions were given that monitoring was to cease where it could not be justified under the *Act*.

Open Sources

CSIS's use of open sources has been one of our continuing concerns. The under-use, rather. By open sources we mean such things as the mass media and scholarly and technical journals, both Canadian and foreign, as an alternative to intrusive investigation. We found, for example, that Australia's ONA draws on information from intelligence sources and also relies heavily on published information, both journalistic and scholarly.

CSIS maintains and adds to open sources in its Information Centre (previously called the Open Information Centre), which provides library and data base search services for CSIS investigations and analysis. But a proclivity for investigative techniques is endemic in CSIS; the Service seems to give more credibility to information it has ferreted out through investigation than to information available to any astute reader.

Our concerns were echoed in the report of the Independent Advisory Team. In one of its few departures from the recommendations we made in our last Annual Report, the Independent Advisory Team did not agree that CSIS researchers should be pursuing independent research or preparing summaries of information on file. But, overall, it supported our view that the Information Centre should be made more relevant to the activities of the intelligence analysts in CSIS. It noted "the Service's apparent hesitancy to exploit open source information to its full potential" and said that "important threat assessments, certainly at the strategic or environmental level, could be completed primarily on the basis of open information".*

* Independent Advisory Team on the Canadian Security and Intelligence Service, *People and Process in Transition*, pages 20-21.

There have been some welcome changes since our last report. Holdings of French-language materials have been increased to 28 per cent of the total—a proportion that library specialists we consulted tell us is excellent for a specialized library of this kind. The increase was not solely aimed at meeting a language quota as such but to ensure that the most useful materials available in French were accessible to investigators and analysts working in both official languages.

Year-to-year comparisons of how much access analysts seek to open information through the Information Centre are difficult because of changes in the way the Information Centre records requests for its materials. But it appears that a sharp rise in the use of the Information Centre in 1987 from 1986 resulted from requests by administrative and technical units. Demand from analysts in the operational branches seemed to drop by almost the same amount, even when figures are weighted to take account of the fact that counter-subversion branch statistics were collected for only part of the year. These statistics, however, do not take into account several open source documents which the Information Centre routinely distributes to the operational branches.

The news from the regions is encouraging. Staff is being trained for regional Reference Centres. We are also encouraged to see that there are now Reference Centres in Montreal, the Ottawa regional office and Toronto, all with up-to-date facilities for accessing data, and that others will open soon in Vancouver and Edmonton. With easier access to open information, investigators in the regions have less reason to use intrusive powers.

Warrant Statistics

There was a significant drop in the number of warrants authorized in 1987 (see Table 1). Part of this reduction is accounted for by the elimination of most counter-subversion warrants, part by the introduction of new warrant authorization procedures following difficulties with the Atwal warrant.

Table 1. New and Renewed Warrants Granted to CSIS, 1985 to 1987

	1985	1986	1987
New warrants	82	94	71
Warrants renewed	27	11	5
Total	109	105	76
Average duration of warrants (days)	173.6	162.2	190.82

Source: CSIS

The statistics in Table 1 follow the pattern of each of our previous annual reports. But in each of those reports we said that we wanted to find a way to provide more precise information about warrants without harming national security.

We have tried to achieve this in a variety of ways, but each new idea has been still-born because of CSIS's sincerely held view that to reveal more would give undue assistance to those engaged in espionage or terrorism.

While we disagree with CSIS, we take the Service's objection seriously, based as it is on national security concerns. Accordingly, we will propose a statistical format that we believe would be useful to Canadians when a Parliamentary Committee commences the five-year review of the *CSIS Act*, scheduled for next year. Parliament itself will then decide whether the *Act* should require the publication of statistics similar to those we will propose, or whether CSIS's national security concerns are sufficiently well-founded to make such action imprudent.

In any event, we can assure Canadians that we will continue to examine all warrants each year, and will immediately inform the Solicitor General and, if necessary, Parliament should there be any misuse, in our opinion, of CSIS powers.

The proposal we will make to the Parliamentary Committee is that the *CSIS Act* require the provision of statistics detailing the number of Canadian citizens or legal permanent residents who have been affected—even marginally—by surveillance powers granted to CSIS under a Federal Court warrant.

Since we believe that to reveal the precise number of non-Canadians affected by warrants could perhaps harm national security, we do not propose to break down the total number of warrants authorized by the Federal Court between those affecting Canadians and those affecting foreigners in Canada. For the same reason, we do not propose to make public the total number of individuals affected by warrants.

In our view, the annual publication of the number of Canadians and legal permanent residents affected by Federal Court warrants granted to CSIS would give the public meaningful information about how CSIS powers were being used, without harming national security. We believe that such statistics would be much more useful than the numbers we have published this year, and would be most unlikely to harm national security. However, we will await Parliament's decision on this issue before making any changes.

Security Screening

The length of time it takes to process applications for security clearances remained a serious problem in 1987-88. It was still taking more than seven months to conduct checks at Levels I (previously called CONFIDENTIAL) and II (SECRET), more than a year at Level III (TOP SECRET). CSIS is the first to recognize that this is too long; it agrees that 30 days would be a reasonable target for clearances at Levels I and II, and the Committee believes that, ideally, 90 days would be appropriate for Level III.

Why are these targets not being met? The explanation is simple: CSIS is swamped. During the year, it dealt with about 90,000 requests to check on prospective immigrants and another 90,000 for checks on applicants for citizenship, 46,000 under the Government Security Policy (GSP), 14,000 for airport workers and 7,000 in other categories.

As intended when the GSP was introduced in 1986, fewer clearances were required under this heading. Requests fell by more than a third from the 1986-87 level. The number of time-consuming field investigations required was also off by a substantial number.

But any hope that this would ease the pressure on CSIS was scuttled by the Department of Transport program to require clearance for all airport workers with access to restricted areas, as a counter-terrorism measure. It was recognized from the outset that these clearances would have to be spread over several years, starting in 1987-88. The first-year target was 10,000. The estimated number of requests in the first year alone is anticipated to be 24,000 to 28,000. Already stretched thin, CSIS was faced with a demand which was 240 per cent of the expected level.

A short-term complication was a rush of major international events in Canada. Nearly 600 Level II clearances were required for the Commonwealth Heads of Government Meeting in Vancouver October 13-17 and about 500 for the Economic Summit that was coming up in Toronto in mid-June, 1988.

Among other problems, the Security Screening Branch is also a victim of the inadequate physical plant provided for CSIS. Analysts are not housed in the same building as records that they must consult. While computer terminals sit in storage because everyone is too busy to see to their installation, Branch employees line up to use the limited number of terminals already plugged in. Many positions in the Branch are vacant.

It is not surprising that, despite the provision of additional resources, a mountainous backlog remained—43,000 citizenship clearances, 33,000 immigration clearances and 15,000 clearances under the GSP. Recognizing that the situation was out of hand, CSIS called in an expert from Treasury Board to see how the system could be streamlined and what further resources were needed. The recommendations contained in the expert's comprehensive report are being implemented and CSIS has shown creativity and flexibility and, indeed, has come up with further improvements to supplement those contained in the report.

An important change is that CSIS's responsibilities in citizenship screening are being streamlined and this will provide a more cost-effective use of Security Screening Branch resources as citizenship accounted for a third of all clearance requests.

CSIS anticipated that by the middle of July, 1988, the entire backlog—including all screening—will be 35,000-40,000 in total, less than half of what it was six months before.

4. Inside CSIS

Our last Annual Report and our special report on staff relations and language issues in CSIS, *Closing the Gaps*, followed by the report of the Solicitor General's Independent Advisory Team . . . all had a major impact last year on the way CSIS conducts its internal affairs. It was not an easy year for the Service, but we see considerable improvements that will make things easier in future. Highlights are discussed in this chapter.

The Academy Revisited

We were encouraged by the decision to reopen the Sir William Stephenson Academy in April, 1988. The Academy is CSIS's own school for training new Intelligence Officers (IOs); it is the doorway through which a new generation is entering the security intelligence field.

We had been deeply disappointed to learn in the spring of 1987 that the Academy would shut its doors for a year. After spending a great deal of money by hiring a large group of intelligence officers at the IO-3 level in autumn, 1986, CSIS said it could not afford to put a class at the lower IO-1 level through the Academy in the 1987-88 fiscal year. What bothered us was that almost all the autumn, 1986, newcomers were ex-police-officers. Entering at a more senior level than Academy-trained recruits from civilian life, they would be in line for faster promotion. It appeared to us that CSIS was missing a chance to diversify the mix of experience and background in its staff.

But in 1987-88, CSIS kept a commitment to stop hiring IOs this way. The only new employees who did not come in through the Academy were middle or senior managers with specific expertise that the Service needed. At the same time, plans were made to provide early retirement for some long-serving officers, which will make room for more new blood.

As to the Academy program as such, we have always been enthusiastic. While much of the transition process, as CSIS took over from the RCMP Security Service, was marked by turmoil and delay, we said in our Annual Report for 1985-86 that "particularly impressive was the speed with which the Service created from scratch a training program that got a very high rating from its first class of recruits". CSIS reaches beyond the security and intelligence community for lecturers at the Academy, into the universities and the Canadian Civil Liberties Association. At year-end, one of our number, Jean Jacques Blais, was scheduled to address the April, 1988 class on our role as a Committee.

Representation and Bilingualism

As the year ended, the April, 1988 class had been assembled. With 12 members, it was very small—the smallest class ever. But it is a step forward, nonetheless. Making the Service more representative of the society it serves is an important objective in recruitment. We find the composition of this class reassuring (Table 2).

With respect to language and sex, these proportions are not as lopsided as they may appear at first glance. They are what CSIS needs if it is to become more representative of the Canadian people. As one of our number, Paule Gauthier, remarked in an address to the Association of Federal Women Lawyers on January 13, 1988, "the realm of national

security is not one where women are much in evidence. History tells us of women who have carried off prodigies of spying, but the number of women in leadership roles at the Service is minimal, if not negligible".

Table 2. Composition of classes at the Sir William Stephenson Academy

Starting Date	Sex		First official language		Source	
	M	F	E	F	Outside	Conversion
Jan 1986	25	8	32	1	33	0
Feb 1986	9	5	8	6	0	14
Jun 1986	16	4	18	2	20	0
Sept 1987	5	2	3	4	0	7
Feb 1987	18	2	14	6	20	0
Apr 1988	4	8	6	6	9	3

Source: CSIS

With respect to first official languages, CSIS also has ground to make up in ensuring that it can operate effectively in both English and French as well as ensuring that it is representative of the Canadian people. We are glad to be able to report that the entire class is bilingual.

With respect to the "source" category in Table 2, the nine recruited from outside the Service are recent university graduates. The remaining three are CSIS surveillance officers "converted" to the IO stream. We have already commented in detail (*Closing the Gaps*, Chapter 15; Annual Report 1986-87, pages 52-53) on the morale problem among surveillance officers—the people who stalk CSIS targets—because their work does not ordinarily lead to promotion. We think it is appropriate that CSIS provide reasonable opportunities for surveillants with the appropriate talents to enter the IO category, with its greater opportunities for advancement.

The representation of ethnic and visible minorities and of native peoples is something that still needs to be seen to. We believe adequate representation of these groups is crucial. It is important that they see CSIS as an environment in which they and their values are respected. And CSIS needs the insights they can bring on the reality of today's multicultural, multiracial Canada. Reliable statistical information on ethnicity is always hard to come by. But casual observation provides ample evidence that ethnic and racial minorities and native peoples are underrepresented in CSIS. Clearly the objective should be to achieve more equitable representation.

We note that the RCMP has created a national recruitment team that, in the words of a March 28, 1988, statement by the Solicitor General, "is carrying the message to minority

and native communities that the RCMP is interested in them for a career in law enforcement". There was already an RCMP campaign to attract francophones and women. The circumstances of the RCMP and CSIS are very different, of course; this is a point we often make ourselves. But we note with interest the RCMP's decision to go out to the people it wants rather than wait for them to come to it. We also note with interest the target of five per cent visible minority representation in the RCMP.

Polygraph Testing: From Bad to What?

The news on another of our recurrent themes gives us some concern. We have repeatedly objected to the use of polygraph examinations within CSIS (Annual Report 1986-87, page 46; Annual Report 1985-86, page 15). We will not repeat our argument in detail here. It is enough to say that even supporters of polygraph testing admit an error rate of at least 10 per cent. The polygraph machine registers the physical manifestations of any kind of emotion; it registers fear or annoyance in exactly the same way as it registers guilt. The "result" of the test is an estimate by an operator who interprets what the machine registers. At best the operator makes an educated guess, at worst a shot in the dark.

We do not necessarily believe that the margin of error is only 10 per cent. But we are prepared to argue on that basis and observe that a one-in-10 error rate would be considered very high in most activities. It is too high to justify the mantle of science that polygraph testing can wrap around arbitrary and damaging decisions about the careers of loyal Canadians.

Last year we were pleased to report that polygraph tests were no longer given as a matter of course to people already on the CSIS staff. But there has been one other improvement in the situation since then. Prospective recruits are now put through polygraph tests for loyalty only. They are no longer given polygraph tests on their lifestyle.

Defenders of these tests make much of the fact that polygraph examination is only one of a battery of screening procedures faced by prospective recruits. True enough. But we do not swallow the claim that an unfavourable polygraph reading is ignored when it is contradicted by evidence from other sources. This does not square with our understanding of human nature in the 20th century, steeped in the belief that "science has the answers". It would be difficult to the point of impossibility for the people responsible for recruitment, with the best will in the world, to give a recruit credit for loyalty to Canada when there is an apparently scientific machine saying something different.

Beyond the damage done to budding careers in security intelligence and the blot left on the record of those who "fail" the test, a larger issue looms. If CSIS and its masters in government see the polygraph as reliable enough for use in the recruitment process, how long will it be until they start using it more widely? Can its use in security clearance investigations be far off? Would the private sector long lag behind government? How long until polygraph examinations were routine for millions of Canadians? That is not the kind of society CSIS was created to protect.

We urged "a thorough and objective study . . . so the Solicitor General and the Government [could] determine for themselves whether such methods [were] compatible with the values of our free and democratic society" (Annual Report 1986-87, page 48).

An interdepartmental committee pursued this issue in 1987-88. It commissioned a review of current research on the matter, prepared by an independent consultant. So far so good. Unfortunately the review shows unmistakable signs of the haste with which we understand it was assembled. It makes no reference at all to the findings of an important Royal Commission in Ontario* that specifically addressed the matter of polygraph testing in the workplace and only passing reference to testimony on 1983 Ontario legislation that bans polygraph testing for screening personnel.**

While the consultant reviews both the pros and cons and does not explicitly arrive at any strong conclusion, we question the objectivity of a report that refers to polygraph examinations as "a form of psychological testing". As a claim to scientific reliability, this description falls on its face when you consider that the people who administer polygraph examinations are not required to be trained psychologists. In fact, CSIS does use trained psychologists to administer its polygraph tests. But the use of trained psychologists is not a universally acknowledged norm that other polygraph users, in or out of government, could be expected to meet as a matter of course.

On the basis of expertise available to us, we take issue with the description of polygraph examinations as "a form of psychological testing" when its procedures lack validity, reliability and comparability and when the meaning of an individual's reactions is assessed on the basis of a procedure that typically lasts only about two hours.

As 1987-88 closed, events seemed to be racing towards a conclusion. The interdepartmental committee had received a report from a working group and outlined options in a paper for the deputy-minister-level Interdepartmental Committee on Security and Intelligence (ICSI). We have not seen either of these documents (they fall outside our oversight mandate). But we hope that ICSI will not reach any decisions whose roots lie solely in the consultant's report, which we have seen and consider inadequate. We hope that ICSI will make further inquiries—in particular that experts in statistical epidemiology will be consulted.

Management

A number of changes have been instituted in the management of CSIS. The Director's office now includes a Secretariat responsible for planning and coordination and for SIRC and Inspector General Liaison, Ministerial and House Liaison, Committee Organization and Support, and TARC. The Director personally chairs all key internal management committees.

One of these is a new Human Resources Management Committee. The personnel function, including official languages matters, is now headed by a full Deputy Director rather than by a Director General, and we are assured that a comprehensive human resources plan is being developed, covering training and professional development, official languages and recruitment objectives.

---

* Mr. Justice Donald Morand, *Report of the Royal Commission into Metropolitan Toronto Police Practices* (Toronto, 1976).

** *An Act to Amend the Employment Standards Act*, Third Session, 32nd Legislature, Ontario.

In *Closing the Gaps*, we urged the temporary creation of a position at the deputy director level to carry out a special official languages plan. In light of developments since then, notably the appointment of the new Deputy Director for personnel and official languages, we have come to the view that this is no longer necessary.

A key personnel issue that we have flagged to the government before is provision for movement between the Service and the Public Service of Canada. Because it would require statutory amendments, it is beyond CSIS's power, and we return to this topic in Chapter 10 below.

As for matters within CSIS's control, it appears to us that the management system is being tightened up in a way that could spare the Service a repetition of some of its past troubles.

5. Counter-terrorism Operations

Counter-terrorism (CT) is one of the two operational branches at CSIS,* and we conducted a thorough study of it in 1987-88. A detailed report is going to the Solicitor General and the Director of CSIS. The report is a long one and its recommendations are classified. This chapter sets out as much as possible of the key findings and conclusions.

CSIS's Mandate

The first issue in other inquiries in this field has been to decide what is meant by "terrorism." One scholarly study cites more than 100 definitions. For CSIS, however, definition is not a problem—its counter-terrorism mandate is set out clearly in paragraph 2(*c*) of the *CSIS Act*—"activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state".

To combat terrorism, like other threats to the security of Canada spelled out in section 2, CSIS has a mandate under section 12 of the *Act* to "collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence" and to "report to and advise the Government of Canada".

It is important to note that CSIS does *not* have a mandate to enforce the criminal law, or to collect evidence for criminal prosecutions. This does not seem to be clearly understood by some of the Service's critics. CSIS seeks to identify the sources and targets of terrorism and other threats to the security of Canada. But protecting the targets and apprehending criminals is clearly the responsibility of the police, notably the RCMP under Part IV of the *CSIS Act* (cited as the *Security Offences Act*).

Our Study: Issues and Methods

We began our study with four questions in mind. First, is CSIS doing its part to protect Canadians against terrorism? To answer this question, we looked into the CT Branch's capacity to identify emerging causes of terrorist activity, to analyse their significance, to gather relevant intelligence, and to transmit timely intelligence to those whose responsibility it is to deal with terrorist threats.

The second question was whether CSIS was working within the law, which includes compliance with warrants and with ministerial instructions as well as with the statute itself. It involves matching the Service's policies and procedures with these controls, and matching field practices with the policies and procedures. It also involves questions of accountability—whether each actor, from field investigator to Director, has the responsibilities suited to his or her place in the reporting structure.

We asked, third, whether there was any unreasonable or unnecessary use of the Service's powers in the CT program. A specific concern was whether the Service's interactions with ethnic communities might influence adversely their political, cultural or social activities.

---

* The second is Counter-intelligence (CI). We will study it in the coming year and include our findings and conclusions in our next Annual Report.

Finally, we inquired into whether the *Act* provides an appropriate statutory framework for CSIS's activities in this area. This issue is timely. Any deficiencies in the CT mandate can be cured next year when the Parliament of Canada reviews the *CSIS Act* (the five-year review is discussed in Chapter 10 of this Report).

The SIRC study entailed: examining the structure of CT Branch, and its financial and human resources; interviewing the CSIS officers who implement the CT program across the country; an examination of the many sources of intelligence used by the Service; reviewing operational files; and reading documents, ranging from the papers which identify developing threats to those which analyze past operations.

We studied the use of resources and intrusive powers by target and by region. We did year-to-year comparisons. We examined indicators of the use of covert means of gathering intelligence and asked how appropriately they were being used against different targets.

The Challenge

The first challenge to counter-terrorism investigations is the difficulty of gathering information. Frequently, terrorist groups are organized into cells—closed, coherent units which resist penetration. It is dangerous to get too close to people who use violence to achieve their objectives. Too close for safety is barely close enough for intelligence gathering. It is said that some terrorist organizations will admit new members to the cell only after they have committed acts of criminal violence. The origins of the information used in CT operations is, necessarily, a closely guarded secret.

Another challenge in CT is change. Terrorist personnel, methods and objectives change over time. The terrorist threats under investigation today were largely unheard of in Canada 10 years ago. Will the threats 10 years hence be those of today? The Counter-Terrorism Branch cannot safely assume that they will be. In addition to investigating today's terrorists, an intelligence service must always be looking ahead to emerging dangers.

The events that could bring future terrorist threats can be happening outside Canada. Most—though not all—terrorist threats to the security of Canada are related to conflicts in other lands. And this is a third challenge for CSIS—to maintain an awareness of events in distant places, events that may reflect centuries of human conflict.

The international character of terrorism brings additional challenges of its own. To the extent that terrorist activity in Canada is aimed at targets that represent, actually or symbolically, the interests of foreign countries, these countries take an interest in potential terrorist activity in Canada. CSIS can benefit from exchanges of information with these countries, but it must guard against two pitfalls. The first is providing them with information that will be misused. The other is accepting at face value false information—"disinformation"—that these countries may offer in hopes of making Canada serve their goals rather than its own.

Increased Priority

The emphasis placed on CT has grown dramatically since CSIS was created in 1984. The Air India tragedy was a turning point for the way Canadians think about international terrorism, and for the CT program at CSIS. On June 23, 1985, an Air India jumbo jet on its way from Toronto and Montreal to Bombay went down off the coast of Ireland, taking all 329 people aboard to their deaths. Most of the victims were Canadians. The Canadian government has not officially determined a cause, but public speculation focuses on terorrist violence.

Faced in the same period with government-wide resource cuts, CSIS management initially tried to meet increased demand for intelligence on terrorism within the CT program as it existed. In some offices, overtime reached levels that were inconsistent with both sound personnel management and efficient use of tax dollars. New programs to enhance the cultural sensitivity of field personnel and to process raw information more effectively were deferred.

But existing resources would not stretch indefinitely, and a new tack eventually had to be taken. CSIS shifted its resources around, moving people and materials into priority CT work. More emphasis was devoted to familiarizing intelligence officers with the roots of ethnic terrorism. The procedures for identifying emerging threats and managing long-term threats were improved. Mechanisms for co-ordinating special events were fine-tuned, and communications with other arms of the government were improved.

These were all improvements. When innocent people are the victims of terrorist attack, the public is entitled to demand the best possible protection. Good intelligence is the first requirement for checking terrorism. So we favour a strong CT program.

Targeting and Investigations

In the study, we examined the targeting policy and procedures laid down in the CSIS Operational Manual, together with all the documents used in making targeting decisions, and we conducted an audit of seven specific targeting decisions. The choice of subjects on our part was largely random. For the warrants which authorize intrusive investigative techniques, such as wiretaps, we checked all outstanding CT warrants, examined some in depth, and reviewed the policy and procedures in the Operational Manual for applications to the Federal Court.

In addition, we made a thorough review of six investigations ranging from long-term monitoring of groups or individuals suspected of making preparations for politically motivated violence, on the one hand, to brief examinations by CSIS of incidents or events with national security implications, on the other.

Targeting and warrant applications are areas where there were dramatic changes in 1987-88 as a result of the "Atwal warrant affair" (see page 14 of this Annual Report). Revisions to the Operational Manual now meet the major concerns we expressed about targeting in our study of the counter-subversion program (Annual Report 1986-87, pages 35-38).

Today, membership in a group suspected of politically motivated violence is not in itself sufficient grounds for targeting an individual in the first instance. Membership in such a group may bring a person to CSIS's attention, of course. But targeting decisions are made on the basis of individual behaviour, and not only group affiliations. We believe this is the proper approach. As we made plain in last year's Annual Report, we do not think people should be targeted solely as a result of being members of groups; targeting should not disregard the nature or extent of their personal involvement.

Although the new policies on targeting and investigation provide all the protections we have advocated in the past, they cause field investigators the opposite concern. Their worry is that, if all their activities must be referable to established threats to the security of Canada, they will be impeded from learning about emerging threats. They should be able to make inquiries—without resort to intrusive investigative techniques—which will permit the Service to discern what their investigative priorities should be in the future. As this Report was being written, the Service was still working out the details of implementing the policies. We urge that a reasonable interpretation be adopted, to permit field investigators to continue the trend towards longer range forecasting of terrorist threats.

We are generally in agreement with the way the CT Branch deploys its resources. With the one exception discussed later in this chapter, the priorities assigned to various terrorist threats are proportionate to the danger they pose. Equally important, Branch priorities take into account impending, as well as immediate, threats. For example, while our study was in course, the Branch, responding to new developments abroad, raised the priority of one form of terrorism that has never produced a violent event in Canada.

The study examined the use, in the CT area, of human sources. The recruitment and handling of human sources is a very delicate business. In addition to the common frailties of human nature, CSIS investigators must concern themselves with motive and reliability.

We found that CT practice as well as policy is to be very careful that sources are directed only against properly designated targets and collect only the kind of information that is properly CSIS's concern under the *Act*. We found CSIS policy on the recruitment of human sources, on source development and on verifying expenditures to be satisfactory, and we found no breaches of that policy.

Our examination of physical surveillance included discussions with officials involved in carrying out this work, a review of the Operational Manual, an examination of internal audits of the program, and a review of all reports about surveillance against CT targets in two regions for a one-month period. We came away very impressed with the competence and resourcefulness of the surveillance operation.

The study looked at the use of technical intercepts, including the processing of intelligence from technical sources. Last December, during the investigation of the Air India tragedy, it was revealed that the Service had erased audio tapes. CSIS operates under a policy which provides for retaining evidence of crime. There is also provision for notifying the police when life-threatening situations are discovered. In general, however, the policy is to transcribe relevant information from intercepts, and then erase the tapes. This prevents

the retention of information about people's private conversations insofar as that information is not relevant to the security of Canada. At the time of writing, we have still not reached any final conclusions regarding tape erasures in the Air India case.

Policies and Practices

Collecting information is what CSIS does best. Our research convinced us that the general quality of the intelligence gathered by the CT Branch is very good. The Branch has a creditable record in tracking the movements and activities of its targets.

It also shows a healthy skepticism about information from foreign intelligence agencies. There are, inevitably, some wild goose chases as a result of inaccurate or misleading information from other agencies; CT is an area where mistakes can cost lives, so no information can be ignored. But the Branch takes into account the foreign policies of countries that supply information and may try to twist Canadian CT activities to their own purposes. It also takes into account the track record of foreign agencies in supplying information that has proved valid—or not—in the past.

In its ongoing investigations, the CT Branch does not intrude unduly in the affairs of ethnic communities. Its attention is focused on clearly established threats to national security, not on entire ethnic groups. We came across one case in which CSIS was repeatedly asked by members of one ethnic community for advice on counter-measures that the moderate majority could use to prevent a minority from manipulating community events for political ends. CSIS's response was restrained and appropriate.

There is a problem with the Canadian chapters of foreign groups which engage in terrorist acts to overthrow the governments of their homelands. Under the *CSIS Act*, the Service is to gather information "to the extent that it is strictly necessary". While the Canadian supporters endorse the objective of the foreign terrorists, their activities here, in many cases, consist largely of political advocacy and protest. Not all conflicts abroad spill over into terrorist attacks internationally.

Where there is no apparent risk of violence within Canada, the Service must take special care to ensure that it is not investigating "lawful advocacy, protest or dissent" except where it is carried on in connection with terrorist threats. It must also be sure to recognize situations where threats are diminishing; that is, as violent conflicts peter out abroad, investigations of Canadian support groups must be scaled back or proportionally reduced. This is particularly necessary in areas such as Latin American conflicts, where the political currents in the homeland are constantly shifting. Our study identified one situation in Latin America where, we concluded, the Service had been slow to shift its attention away from such a group as the group's contribution to the conflict abroad dwindled. Although the targeting of the members of the group is lawful under the *Act*, we felt the scope of the investigation was exaggerated.

We also have some concern about the possible by-products of Service activities in connection with special events like the Commonwealth Heads of Government Meeting. In

advance of such events, the CT Branch interviews mainstream members of ethnic communities that have terrorist elements on their fringes. Its purpose is to gather information about potential threats.

But there is another, incidental effect: these interviews remind everyone in the community that CSIS is watching and, thus, warn off extremists. It is all to the good if terrorists are deterred. But we fear that the inhibiting effect could extend throughout the community concerned if the practice is not controlled. Feeling that they are under the eye of the authorities, other members of these communities could be discouraged from exercising their rights of legitimate and lawful dissent. This is a continuing dilemma for the Service requiring careful and continued attention each time there is a "special event".

Intelligence Production

Under section 12 of the *CSIS Act*, the Service's core role is to provide intelligence and advice to the government. We checked with a number of federal agencies that are the principal consumers of CT intelligence and found that they are generally satisfied with the quality of the intelligence they get on terrorist threats. They are also generally satisfied with their access to CT personnel to discuss issues and problems. Information given to consumers on how to identify suspected terrorists is well received. So are analyses which describe the level of danger to particular interests from particular terrorist organizations.

A continuing problem is the different approaches of CSIS and the police to terrorism. CSIS believes that, in certain cases, the police would like the Service to use its investigative powers in support of the police role, which is law enforcement. But this is not what CSIS was created to do. It was created primarily to provide advice on the basis of its analysis of information from both open and covert sources. Of course it has a duty to assist the police when and where it can. But its emphasis belongs on gathering information over gathering evidence in a form that can be used in court. CSIS has done its job when it has pinpointed a threat and told police about it. It should not then endanger the effectiveness of its procedures in order to accumulate evidence that can be used in laying charges and securing convictions.

Co-operation between CSIS and the RCMP has improved considerably. This is due in no small part to the exchange of Liaison Officers between the two agencies. The differences in emphasis between intelligence and evidence inevitably continues to cause some strain. CSIS insistence on protecting its sources sometimes leaves the police wondering whether they are getting all the information they would like.

In our own examination, we found that the CT Branch is at its best in dealing with current threats. It is an operational branch and most of its intelligence products serve immediate operational purposes. The Branch also produces assessments of long-term trends in countries from which there is no immediate threat to Canada. While this is probably the least important product of the Branch, these assessments are not up to the standards of the intelligence produced by the Analysis and Production Branch, discussed in the next chapter.

The same unit which carries out research within the CT branch also prepares briefings for senior officials, notably the Director of CSIS. The briefing function, with its more immediate deadlines, tends to displace the intelligence function. We think it is good that

the Director meets personally with other parts of the intelligence community and naturally he must be well-briefed for such meetings. But we do not think that briefings and operational research co-exist well in the Research and Briefing Unit. Each has an important role in the CT Branch. We would like to see these roles expanded—and separated.

If the Director gets around, operational analysts in the CT Branch do not. They are given few opportunities to attend national or international meetings on terrorism. We think they should be given more opportunities to meet with their counterparts and colleagues in other countries so each understands the other's work better and, when events are developing quickly, there are personal as well as working relationships to help oil the machine.

Conclusion

At the end of our study, we were broadly satisfied with the answers we found to the four questions we started with. We found that the CT Branch provides adequate protection to Canadians. It stays within the law. The *CSIS Act* provides a suitable framework, dividing CSIS's intelligence role from the law enforcement role of the police.

In the Counter-Terrorism Branch, CSIS is showing that it can gather information in a forward-looking manner which goes beyond supporting law enforcement activity.

In areas where the Branch has historically been weak, such as analysis, we discerned pronounced improvement. The areas where the need for further improvement is greatest are in long-term strategic analysis, which we discuss in the next chapter of this Annual Report.

6. From Information to Intelligence

Information is the raw material that CSIS works with. The finished product is intelligence—information sifted and arranged in such a way as to help users make the right decisions. CSIS has an Analysis and Production Branch (APB)* whose job, in the words of the Operational Manual, is "to produce intelligence assessments in concert with the operational branches and facilitate the flow of information to the relevant decision makers in the Government of Canada".

APB produces papers called *CSIS Reports*, each summarizing current intelligence on a single topic, organization or person, and special reports that go into more depth. It also contributes papers and information to the Intelligence Advisory Committee (IAC) and the Security Advisory Committee (SAC). These are the key subcommittees of the deputy-minister-level Interdepartmental Committee on Security and Intelligence (ICSI) which reports, in turn, to the Cabinet Committee on Security and Intelligence, headed by the Prime Minister. Overall, APB output exceeds 250 documents a year.

We conducted a review of the intelligence analysis and production process in APB in 1987-88. But CSIS is not alone in this field; the Departments of External Affairs and National Defence, to take the most obvious examples, have significant capabilities of their own, and many arms of the federal government make use of security intelligence. So our inquiries inevitably led us to consider CSIS's relationships with other agencies, both producers and users.

In carrying out the review, we met with APB staff at all levels—the Director General of the Branch, present and former section chiefs and a number of working analysts. We followed some draft *CSIS Reports* through the process, looked at work done for IAC and sat in on the deliberations of the APB Intelligence Production Committee. We also had discussions with other agencies that use CSIS intelligence, studied the training, experience and academic qualifications of APB analysts and reviewed the relevant scholarly literature. We drew on a user survey carried out by the Branch itself in 1987-88.

A full report is going to the Solicitor General for his consideration. This chapter reviews key findings and issues.**

The Intelligence Product

We adopted the distinction made by the Solicitor General's Independent Advisory Team between operational and strategic intelligence.*** *Operational intelligence* is "related to the investigation of particular activities considered threatening to the security of Canada". It "relies heavily (but not exclusively) on investigative techniques, is usually short-term and is produced for specific consumers or for a specific purpose". This is "case-oriented" intelligence, and CSIS itself is a major consumer as well as a major producer. Operational intelligence is the province of the operational branches of CSIS, Counter-terrorism and Counter-intelligence, and they have their own staff analysts.

---

* Formerly called the Intelligence Assessments Branch (IAB).

** APB also keeps a watching brief on low-level counter-subversion targets (see Chapter 3 above), but our study focuses on the assessment and production process as such.

*** *People and Process in Transition*, pages 18 and 39.

APB produces *strategic intelligence*. This intelligence "relies more heavily on research using information from all sources, tends to be longer term and more global in scope and is produced for an interdepartmental audience or for the government as an entity". It "is evaluated in the context of other Canadian national interests". Within the strategic category, we distinguish current from basic intelligence. *Current intelligence* focuses on events as they unfold and alerts decision-makers to potential emergencies. *Basic intelligence* is in-depth data on countries and subjects, which should help the government in the development of policy and in strategic decision-making.

To illustrate with the example of a meeting between two individuals suspected of being threats to the security of Canada, operational intelligence would determine that the meeting took place and report, if possible, what was said. Current intelligence would put the meeting in context—identifying what organization these people belong to, for example, and suggesting what this meeting may reveal about possible changes within the organization and its plans. Basic intelligence provides the larger context by assessing the capabilities, intentions and vulnerabilities of the organization.

Current intelligence accounts for most of APB's production. This is reflected in comments by users that what *CSIS Reports* do is alert them to specific issues—weapons sales, for example. We see a gap; the government is not getting all the basic intelligence it needs. A steady stream of current intelligence reports can result in security intelligence being dealt with as a series of "flaps" rather than as an ongoing, long-term process.

Setting Priorities

The reasons for APB's emphasis on current intelligence can be found partly within CSIS itself. But the ultimate responsibility for determining intelligence requirements and setting priorities lies not with CSIS but with the government. It is a common criticism in the security intelligence field throughout the Western world that governments do not give their intelligence agencies clear enough direction, and this appears to be true in Canada.

In the absence of clearer direction from the government, a number of factors within CSIS have encouraged the emphasis on current intelligence. One stated by CSIS officials we spoke to is the inexperience of much of the APB staff. About half the Branch's analysts are newcomers to security intelligence since CSIS was created in 1984, and they are cutting their teeth on short-term, current intelligence projects. More experienced analysts are deflected from basic intelligence production by the need to spend time guiding their juniors. This, we were told, will change as experience grows.

Perhaps so, but there are also entrenched institutional factors. For one thing, APB does not have a unit devoted solely to producing basic intelligence. More far-reaching is the influence of the operational branches over APB.

A major role in setting APB's program is played by the operational branches through the Intelligence Production Committee (IPC) within CSIS. IPC is headed by the director general of APB, but the directors general of the operational branches have most of the votes. There is a higher level "executive" IPC of deputy directors which ought to be providing a

broader perspective, but it is largely inactive. It met only once in 1987. The director-general-level IPC (which is what we mean by "IPC" in the remainder of this chapter) has naturally filled the vacuum.

After determining where APB analysts will focus their attentions, IPC comes into the picture again at the end of the production process when it comments on the final draft of each report, may order revisions, and decides on distribution to client departments and agencies, to CSIS security liaison officers abroad and to friendly foreign security and intelligence agencies.

Sources and Methods

Analysis relies on a number of sources—information gathered in investigations by operational branches, the security liaison officers, open information such as the mass media and publications by experts, the security and intelligence agencies of friendly countries, and other parts of the Canadian intelligence community.

The influence of the operational branches continues after a topic for analysis has cleared IPC. The APB analyst often works closely with a counterpart in the relevant operational branch. Much of the raw information used by the APB analysts is from operational sources. The operational officers often check the APB conclusions. The resulting paper sometimes goes to the director general of the operational branch for review before it reaches the APB analyst's own chief and the APB's own Review Committee.

A more subtle influence, at least for the immediate past and the immediate future, is that many of the APB analysts have less experience and less status than their operational counterparts. In addition, most APB analysts are attached to operational branches. They even have their offices in the quarters of the operational branches they work with instead of being all together, so the corporate culture they absorb from their surroundings is operational rather than analytical. In one section, the Chief's office is in a different building from the offices of most of the analysts under him.

We were glad to find that APB's reliance on open sources is growing. Readers of our annual reports will recognize maximum reliance on open information as one of our signature themes (see, e.g., page 17 of this Report). Our inspection of user data for 1986-87 and 1987-88 showed a 10-per-cent increase in APB requests for open data from the CSIS Information Centre.

We have also had occasion in the past (Annual Report 1986-87, page 23) to remark that CSIS might be too ready to accept information supplied by friendly agencies in other countries at face value. We were told in our APB review that analysts cast a critical eye on information from allies with axes to grind on specific issues. In addition, corroboration from other sources was a criterion in assessing information from other agencies; in theory, such information should not be accepted before it is confirmed elsewhere.

But confirmation is not always easy, and APB section chiefs do not have enough access to computer terminals that would let them double-check source documents. Incidentally, this and other inadequacies in physical arrangements are small but telling signs of inadequate

day-to-day attention at the top to the Branch's work. In our discussions with intelligence users, the point was sometimes raised that *CSIS Reports* did not always pay sufficient attention to Canadian implications. Other users, however, stated that APB efforts to put more emphasis on "Canadian considerations" are apparent.

As to analytical procedures, no models have been set by APB for its analysts to follow. IAC and SAC expect work done for them to be in a specified format. But, generally speaking, APB counts on each analyst to select a framework suitable to the matter in hand. We do not suggest methodological strait-jackets in which the facts are selected to fit the format instead of the format being shaped by the facts, but we are concerned that the absence of ground rules makes it difficult to assess analysts' work. A middle way needs to be found.

New APB analysts follow a special course at the Service's Sir William Stephenson Academy, but it focuses on operational analysis. It does not encompass political and strategic analysis. This is a gap that must be filled quickly. There is a consensus among APB managers that more specialized intelligence assessment training should be available, and we hope that discussions now underway will soon bear fruit.

Specialization

We also have some concern about obstacles to the development of world-class expertise within APB over the years. The prevailing view within CSIS is that analysts should be generalists, not specialists. We see advantages in this approach. It lets the analysis function adjust more quickly to changing priorities. It encourages fresh thinking as a wide range of knowledge and experience are brought to bear on topics.

But these advantages are vastly outweighed in our view by the need for in-depth knowledge. Generalists are less likely, for example, to be attuned to the cultures of the group they are studying. They will be ill-protected from thinking in stereotypes and less able to pick out significant nuances.

The bias to generalization is more than a matter of attitudes within CSIS. It has strong organizational underpinnings that will perpetuate it indefinitely unless there is a clear and specific decision to encourage specialization.

Analysts rank in the "journeyman" IO-1 to IO-3 levels in the job classification scheme. Once they have reached the IO-3 level they may have difficulty moving into entry-level positions in the operational branches. Yet they can advance no further within APB unless they become managers rather than analysts. This eliminates the hope of higher pay and higher status as a reason to do the independent study that specialization requires under present circumstances. In addition, the present classification levels are not likely to attract specialists from other branches or from outside the Service.

We think that there should be senior—specialized—analysts classified above the IO-3 level. In this connection, we think APB could be a good place to locate suitable CSIS liaison officers when they come home from assignment abroad. Intelligence production could benefit greatly from their extensive experience. But they hold ranks well above IO-3, so APB is not now an attractive destination for them.

Two other institutional constraints on specialization are discussed in a broader context in Chapter 10, so we will simply mention them here. Members of CSIS are encouraged to remain publicly anonymous, so they seldom present papers at conferences. Indeed, the Branch does not have sufficient resources even to send analysts to conferences. (CSIS does, however, have an in-house program of seminars and presentations involving people from other parts of the security intelligence community, Canadian and foreign). Second, there are statutory obstacles to transfers and secondments between CSIS and the Public Service.

Meeting User Needs

It is a welcome sign of Branch management's commitment to improving its product that it conducted an extensive survey of users in 1987-88. We found it a useful supplement to our own interviews with users. We are not as impressed with the user questionnaire circulated with each *CSIS Report* which invites superficial responses. We are also concerned that the Branch does not systematically evaluate its own work in light of subsequent events, and we urge that it start doing so.

Nonetheless, and despite some criticisms, the consensus within the security intelligence community is that the assessments provided by APB are getting better. We found that there was still too much description and not enough analysis, but APB's efforts to right the balance and to focus more on the "Canadian implications" section of its reports are also evident. APB acknowleges the justice of complaints that its conclusions need to be better substantiated.

Timeliness was one problem flagged by users; they said they were not getting *CSIS Reports* quickly enough. Urgent briefs and reports are distributed electronically for the sake of speed, but a degree of slowness is built into the system. Part of the blame must go to a cumbersome approval process for APB papers. As more analysts gain more experience, it should be possible to bypass the Review Committee composed of APB chiefs; each chief could take responsibility for the work of the section and send it directly to the IPC. At the least, the Review Committee needs to be given formal terms of reference.

Translation delays are another problem. A 1- to 3-page document takes no less than a week to translate. Documents of more than 20 pages require four weeks or more. APB could speed the process itself by following the common practice of sending an early draft to translation, so there are only revisions to be made when the document is in final form. However, as we have in other contexts, we also urge CSIS to make sure it has enough translators to meet the demands of government-wide official languages policy.

Some users said that the classification of *CSIS Reports* as SECRET limits their usefulness, since they could not be given without censorship or special dispensation to some people who could benefit from them but did not have the required security clearance. Liaison was also identified as a problem by some users; APB recognizes the need to brief users directly on some issues of special concern to them, to ensure that the implications of the intelligence provided are drawn out and that user needs are well understood.

Options for the Future

Among our key findings were an emphasis on current rather than basic intelligence and, in the absence of clearer direction from the government, the great influence of the operational branches on APB. These two matters are related. The operational branches raise issues for analysis, influence its production through the information they provide and through formal reviews, and ultimately decide what will be circulated.

CSIS management needs to consider whether it wants to maintain the status quo, producing mainly current intelligence under strong operational influence, or give APB the resources and organization it needs to develop more basic intelligence. In either case, we believe that IPC should have proportionately fewer members from the operational branches and more from APB itself. Drawing on its perspective as a service to the government as a whole, APB needs to have more influence over its own analysis priorities and over the content of the intelligence that it disseminates.

Another option for consideration by the Government would be the creation of a separate assessment agency on the Australian model to produce basic intelligence. Such an agency would not replace APB, which would continue to produce current intelligence. The overlap with present Canadian structures would be more with IAC, though it acts as a clearing house and coordinator rather than as an intelligence producer.

When we visited Australia, we paid particular attention to the role of the independent Office of National Assessments (ONA) there. The Australian Security Intelligence Organization (ASIO), which corresponds with CSIS in Canada, collects and distributes information and analyses intelligence principally from an operational point of view. ONA is an assessor, not a collector, and it is an external agency, not an internal one. That is, it does not collect intelligence but uses intelligence and other information, including from open sources, to produce reports, appreciations and assessments, and it is directed not to the internal security of Australia but to international, political, strategic and economic matters of relevance to Australia.

Australian officials are convinced of the value of independent intelligence assessment. Away from, though not unaware of, the urgent demands of day-to-day operations, ONA can concentrate on long-term requirements. There is little temptation to expend resources on "data-driven" work—that is, analysing whatever happens to have been turned up through investigations by the collecting agencies. Studies are "need-driven". They must be directed to a clear objective and have at least the potential for leading to recommendations for specific government action. In fact, as a full member of the Secretary's Committee that serves the cabinet and also through its assessment of where problems are likely to arise or where available information is too sparse, ONA plays an important role in setting priorities for the collecting agencies, including the Department of Foreign Affairs and Trade, whose normal diplomatic reporting is a prime source of ONA's information. ONA is the institutional critic of the quality and quantity of information the collecting agencies provide.

ONA's access to expertise also impressed us. Most ONA analysts have post-graduate degrees and they rarely remain on staff more than five years, so there is a constant infusion of the latest knowledge and thinking from the worlds of scholarship and the professions.

We want to make it clear that we are not at this point recommending imitation of the Australian model. We have not had an opportunity to examine this matter thoroughly enough for that. We also recognize significant differences between APB's role in CSIS and ONA's role in Australia. But we believe a separate agency is an option the Government might consider if it shares our view that it needs more basic intelligence.

Summing Up

Before CSIS was created in 1984, the history of assessment units in Canadian security intelligence was a record of failed starts. That has changed. We found that APB is moving more and more towards producing the kind of intelligence that SIRC believes the government needs.

Branch managers have taken important initiatives to ensure that their product becomes as good as it can be under present circumstances. We have mentioned the user survey, which was carried out well. Memoranda of understanding have been signed with the operational branches, to ensure that the division of responsibilities is well defined. APB has won the respect of the operational branches and, with it, the access it needs to sensitive information held by these branches.

However, APB can only go so far on its own. In particular, Service-wide personnel policies are an obstacle to hiring and developing specialists with an intimate understanding of the social and cultural backgrounds of CSIS targets. Service management's undoubted commitment in principle to analysis and production does not seem to be followed through day to day.

We believe that Canada will only get the best strategic intelligence possible when APB enhances its corps of professionals in order to produce policy-relevant analyses. They should draw on the whole range of information available to the government and rely less on the product of field investigations. If such a group does not fit within CSIS, the Government could consider creating one elsewhere.

7. Complaints

As we have already explained, we have a dual mandate under the *CSIS Act*—oversight and complaints. Paragraph 38(*c*) of the *Act* directs us to investigate complaints that anyone may make about the activities of the Service and complaints about the denial of security clearances in Public Service employment, in the supply of goods and services to the Government of Canada and in immigration and citizenship matters. We also investigate the security aspects of certain complaints lodged with the Canadian Human Rights Commission.

Summary case histories of investigations completed in 1987-88 can be found in Appendix B of this Report. In this chapter, we provide an overview and discuss current issues in the complaints process.

The 1987-88 Cases

We took in 38 new complaints in 1987-88—exactly twice as many as the year before (see Table 3 below). Complaints about the denial of security clearances and about security considerations in immigration remained at 1986-87 levels, one and two respectively. Complaints about an intention to deny citizenship for reasons of national security or involvement in organized crime fell to one in 1987-88 from two the year before.

But the number of complaints under section 41 of the *Act* rose by a factor of 2.6. Section 41 provides that "any person" may lodge a complaint "with respect to any act or thing done by the Service". We must investigate if three conditions are met—first that the Director of CSIS has already had a chance to deal with the matter, second that we are satisfied the complaint is not "trivial, frivolous, vexatious or made in bad faith" and, finally, that there is no other avenue of redress under either the *CSIS Act* or the *Public Service Staff Relations Act*. These complaints numbered 34 in 1987-88, compared with 13 the year before.* We also carried two such cases over from 1986-87.

There was no pattern in the nature of the section 41 complaints. The increase simply seems to reflect growing public awareness of our Committee and its work rather than any particular failing on CSIS's part. Thirty complaints could be dealt with quickly; either they were clearly out of our jurisdiction or the complainant offered no factual base on which an investigation could proceed. We completed the investigations of two complaints. In neither did we find any wrongdoing by CSIS.

In one security clearance complaint, we recommended that the clearance be granted. It is too early to know whether our recommendation will be accepted. Among the citizenship cases, three files were closed before we completed our investigation, because CSIS withdrew its objections. We agreed in the fourth case that citizenship should be withheld. In immigration, we agreed with deportation of one individual and in a second case, which involved criminality, the file was closed before investigation was completed because the RCMP withdrew its objection to the individual's entry into Canada.

---

* In this discussion, we do not take into account more than 2,000 complaints made by CSIS employees in 1985-86 and 1986-87 about the official languages practices of the Service. These complaints have been dealt with through a special inquiry, which we published in 1986-87 under the title *Closing the Gaps*.

As can be seen in Table 3, we closed 39 complaint files in 1987-88. With 14 files carried over from the previous year and 38 new complaints, this left us at year-end with 13 files open. This is a manageable number—one less than we had at the same time a year earlier.

Table 3. The Complaints Record, 1987-88

	New complaints	Carried over from 1986-87	Closed	Carried over to 1988-89
Security clearances	1	1	1	1
Citizenship	1	7	4	4
Immigration	2	4	2	4
Section 41	34	2	32	4
Total	38	14	39	13

Who Decides?

An issue of great long-term significance came to a boil in 1987-88 when the Federal Court of Appeal stated as *obiter dicta* in *Thomson v. The Queen* that deputy ministers are bound by our recommendations on security clearances in Public Service employment; when we conclude after investigation that a clearance has been unreasonably withheld, the deputy minister concerned must act on our recommendation to grant that clearance.* Continued refusal could, the Court said, be justified by new information that came to light after our investigation was completed. But such a refusal could, of course, give rise to a new complaint for our adjudication.

However, no one expected that this would put an end to the question. Nor did it. For jurisdictional reasons, the same matter came before the Trial Division of the Federal Court for decision soon afterwards, and the ruling went the other way; deputy ministers are not bound by our recommendations, said Mr. Justice Dubé of the Trial Division.** Now this decision is under appeal.

The matter arose in this way. Robert Thomson was the successful candidate in a competition for a position in the Department of Agriculture. The position required a security clearance at the SECRET level (now called Level II), so his appointment was conditional upon his receiving this clearance. After making inquiries at the request of the Department, CSIS recommended against clearance. A number of allegations against Mr. Thomson are

* Unreported decision of the Federal Court of Appeal, March 7, 1988.

** Unreported decision of the Federal Court of Canada Trial Division, June 15, 1988. This decision came down after the end of the year covered by this report, but we feel it is necessary to take note of it here; to do otherwise would give a very misleading picture of the situation.

on the record, including the fact he "leaked" at least one document that came his way when he worked for the Canadian International Development Agency some years ago. After consulting both his own officials and the Privy Council Office, the Deputy Minister denied the clearance and the offer of employment was withdrawn.

Mr. Thomson thereupon complained to us. In accordance with our normal procedures, two of us conducted an investigation. Mr. Thomson, the Department and CSIS were all represented by counsel. The conclusion was that Mr. Thomson "would be unlikely to release classified information if he were once again employed in a position with access to such material". We recommended that Mr. Thomson be granted the SECRET clearance so he could take up the position. The Deputy Minister stood by his original decision, and Mr. Thomson applied for relief to the Federal Court of Appeal.

That was when the Court of Appeal said that the Deputy Minister did not have a choice in the matter: he was bound to follow our recommendation. But the Court did not have jurisdiction to set aside the Deputy Minister's decision, as such orders are the prerogative of the Trial Division. Mr. Thomson accordingly turned to the Trial Division, bringing Mr. Justice Dubé's ruling.

Until the Courts have ultimately disposed of this case it would be inappropriate for us to comment further on the merits of the legal issues involved.

Disclosure

We have an on-going tug-of-war with CSIS over the disclosure of information to complainants. Recognizing the Service's responsibility for guarding national security, we are always reluctant to give complainants information against its advice. But we have a responsibility to ensure that complainants know enough to make an informed response to allegations that have been made against them.

Section 46 of the *CSIS Act* sets out this duty with respect to the denial of security clearance in government employment and government contracts. It says we must give the complainant "a statement summarizing such information available to the Committee as will enable the complainant to be as fully informed as possible of the circumstances giving rise to the denial of a security clearance". In principle, the complainant should have all the relevant information available to us, subject to the "as possible" limit. The principal constraint we accept in providing information to complainants is that CSIS sources must be protected from exposure. There are similar provisions with respect to citizenship and immigration complaints.

In both Australia and New Zealand we were told that disclosure is not a problem. The president of Australia's Security Appeals Tribunal said that the Australian Security Intelligence Organization, which corresponds to CSIS in Canada, is generally cooperative about providing complainants with enough information to permit a full defence. In New Zealand, Sir Thaddeus Pearcey McCarthy, the Commissioner of Security Appeals, told us that he always gives complainants all the details of the allegations consistent with concealing sources.

Here in Canada, we have found that CSIS is overly cautious in its view of how much complainants can be told, and we have often had to take a strong stand. CSIS still finds this process disorienting. In one case, CSIS withdrew its objections to citizenship for an individual rather than have us reveal information that we thought the person needed to mount a reasonable defence.

8. Inside SIRC

Our operational activities in oversight and complaints have been described in the foregoing chapters. Still to come are chapters on two broad issues that transcend the daily grind—our work to foster informed public discussion of security and intelligence issues and, second, some matters that Parliament and Canadians may want to consider when the *CSIS Act* is reviewed in 1989. In this chapter we put some housekeeping details on the record.

Our Work as Members of SIRC

Much of the day-to-day work of our Committee and much of the research is conducted, of course, by our staff. But we are all personally active in the oversight and complaints process. We meet as a Committee at least monthly to discuss issues and make key decisions. We work individually with staff on such projects as the counter-terrorism study reported in Chapter 5. Hearings on complaints are conducted by us in person, but with hearing panels usually of one or two Members established by the Chairman to spread the work around.

We continue to believe that there is value in having a part-time, all-party Committee like ours to provide oversight and investigate complaints. The tri-partisan nature of the process by which we are appointed under the *Act* is an assurance to Parliament and the public of impartiality. Yet it has not been an impediment to the collegial approach we have taken to our work. The fact we are not permanent officials is also valuable. Being active members of our communities in different parts of the country probably helps maintain the degree of detachment appropriate to an oversight body.

Financial Report

Our 1987-88 spending is set out in Table 4.

Table 4. SIRC Budget 1987-88

Personnel		$565,000
Salaries and wages	$491,000	
Contributions to employee benefit plans	$74,000	
Goods and services		$661,000
Professional and special services	$507,000	
Other	$154,000	
Total operating expenditures		$1,226,000
Capital expenditures		$9,000
TOTAL		$1,235,000

Source: 1988-89 Estimates, Part III

Personnel

Our staff still stands at 13, headed by an executive secretary who directs all day-to-day operations. Other employees are a research director, two research officers and a research assistant, a senior complaints officer, an executive assistant who supports our research and complaints functions, an administration officer who doubles as registrar for our hearings and triples as coordinator of our responsibilities under the *Access to Information Act* and the *Privacy Act*, a records officer, a records clerk and three secretaries.

9. Need to Know

One of the most-used phrases in security and intelligence is *need to know*. In CSIS and its counterparts worldwide, information is relayed on a need-to-know basis. Each fact, each idea is imparted only to those who need it to carry out their work. Everyone else is kept in the dark. Thus the risk of leaks is lessened—and the circle of suspects is limited if a leak does take place.

There is another need to know—the public's need to know what is being done in its name. Many details of security and intelligence work must, of course, remain secret for the obvious reason: publicity would arm democracy's foes. But much can be told without danger to national security, and it should be told.

Intelligence Directory

We mentioned last year that, when SIRC was created, we found many of our questions were not readily answered from available materials. For example, as newcomers to the world of intelligence, we wished for a comprehensive directory of federal agencies engaged in security and intelligence.

All the agencies helped us to compile that directory ourselves. It has proved useful for other newcomers, including CSIS recruits.

We have now produced an expurgated version for public consumption and are publishing it as Appendix C of this Report. We caution that it is purely descriptive; nothing in it is to be taken as an assessment of the various organizations it describes.

Reaching Out

The directory is one example of a conscious effort to increase public understanding of security intelligence issues and to make CSIS's work better known. The annual report is our major vehicle. We prepare it primarily to meet a statutory obligation, of course, but we are also conscious of the contribution it can make to informing Parliament, academic and other specialists, the media and (largely through the media) the Canadian people. In the absence of any other open source, it provides the only statistics available to Canadians generally on warrants granted to CSIS. It has let us keep debate going on issues like the use of open sources and targeting procedures.

The annual report forms the basis for appearances before Parliamentary Committees. During the year under review, we appeared before the Standing Committee of the House of Commons on Justice and Solicitor General on December 17, 1987 (with a second appearance shortly after the turn of the fiscal year, on April 14, 1988).

As explained in Chapter 2 above, we also make special reports to the Solicitor General, and some of these are made public. Our special report on *CSIS' Use of its Investigative Powers with Respect to the Labour Movement* was released in March, 1988 (see Chapter 3 above for a review of key findings). Last year, we published *Closing the Gaps*, an abridgment of our report to the Solicitor General on official languages practices and staff relations in the Service.

Another important vehicle for public information is our speaking engagements before interested publics. The Chairman, Ronald G. Atkey, delivered a paper on "Accountability for Security Intelligence Activity in Canada" on May 8, 1987, at the Osgoode Hall Law School conference on Domestic Security: Issues for Democracy. Jean Jacques Blais spoke with political science students at Carleton University in Ottawa last fall, while Paule Gauthier touched on the work of our Committee in an address to the Association of Federal Women Lawyers in January, 1988, and addressed the Political Science Department at Laval University in Quebec this spring. As the year ended, Mr. Blais was preparing an address on "the Political Accountability of Intelligence Agencies—Canada" to the 1988 conference of the Canadian Association for Security and Intelligence Studies.

We are frequently in touch with the media, which look to us for information and background when security intelligence stories erupt. We held a news conference when our last Annual Report was tabled in June, 1987.

Canadian Scholarship

We have also acted on the need we see for Canadian scholarship in security intelligence issues. So much of our knowledge and thinking about these matters in Canada has been based on the study of American and European experience.

Back in 1985, wanting to prepare ourselves for our responsibilities in launching SIRC, we sponsored a seminar where about two dozen scholars in relevant disciplines and other experts shared their knowledge and their perspectives with us. Some of the issues we discussed back then are still at the heart of our approach—our concern for striking a balance between the protection of fundamental freedoms and effective intelligence gathering, for example.

This year we participated in the sponsorship of two conferences. The Centre for Public Law and Public Policy at Osgoode Hall Law School put on a conference at York University May 8-9, 1987, on Domestic Security: Issues for Democracy, which we underwrote. Then we shared sponsorship, with the Office of the Inspector General, in a conference on Advocacy, Protest and Dissent at Queen's University in Kingston February 25-27, 1988. There is no need to review the proceedings of these conferences here as they are to be published—except to say that they made an important contribution to the goal of informed debate.

Members of our staff sometimes make individual contributions. One of our researchers presented a draft paper at an international colloquium staged at the University of Seville in Spain February 25-27, 1988.*

He quarrels with the view that without media attention, terrorism would wither away. When, for example, authorities buckle under pressure to save innocent lives, sometimes in

* M. Klein, *Terrorism and the Media: A Social Learning Approach*, a draft paper presented to the Ninth International Colloquium on the Brain and Aggression, University of Seville, February 25-27, 1988. Views expressed in this paper are the author's, not necessarily the Committee's, but we agree with the views cited in this Report.

the face of negative international publicity, terrorists are confirmed in their view that violence gets results. Bonding within the terrorist cell and the "heroic" standing that the individual terrorist enjoys among sympathizers also give terrorism a life of its own.

But modifying the behaviour of the immediate targets through aggression and violence is seldom the whole terrorist agenda. By courting media coverage, terrorists seek to spread their propaganda, to demoralize the public and the authorities, for example, or to appeal to new sympathizers and awaken potential recruits.

Media: Friend, Foe . . . or Both?

Clearly the media play a key role in the contemporary rise and spread of terrorism and in the way individual acts of terrorism unfold. In general, the mass media are a positive force in fostering informed discussion of security and intelligence matters. There is no other institution in society with their reach and their ability to present issues in terms that most people can understand. But we are not blind to the problems that can arise in reporting on terrorism and on security intelligence generally. In the opening chapter of this Report, we commented on the atmosphere of suspicion that swept the Canadian media in the wake of some real CSIS problems, leading to some questionable reporting. And when terrorists earn points simply by making news, then reporting news about terrorists is a minefield.

Specific instances in Canada of conflict between the public's right to know—which is served by the media—and legitimate security requirements have been documented by the Senate Committee on Terrorism and Public Safety.* Instances abroad are well known—the "Beirut Syndrome", for example, in which major media go along with terrorist conditions on the dissemination of information.

It is not realistic to expect the media to stop reporting on terrorism. It is not desirable, for the public needs to know how the game of politics is being played, whether by fair means or foul. But we readily endorse the observation in *Terrorism and the Media: A Social Learning Approach* that "it is important that reporters be sophisticated enough to realize when and how they are being manipulated by terrorist movements". Sometimes the issue is simply one of timing: does the public need a breathless live report the minute the SWAT team moves into position or can it wait a few hours? Sometimes the issue is more complex: should reporters accept the role—as some Irish reporters have—of uncritical conduit for terrorist propaganda for the sake of the nuggets of exclusive information that come their way as a result?

Speaking Up for CSIS

Another aspect of the public's need to know is its need for a realistic picture of CSIS. We accept some responsibility. Our Executive Assistant stressed realism when she spoke to the Centre for Investigative Journalism at its 10th annual conference in Toronto, March 25-26, 1988. James Bond is fun but fiction, she said. "The truth would be better served if the

* Senate of Canada, *Report of the Special Committee of the Senate on Terrorism and Public Safety* (Ottawa, Supply and Services Canada, 1987).

cloak-and-dagger symbol for espionage were changed to that of a typewriter and some 3x5 index cards."

CSIS itelf has a responsibility, of course. We have previously urged (Annual Report 1986-87, page 46) that it undertake a public relations campaign designed to foster an appreciation among Canadians of its role. We saw this primarily in staff relations terms, as a means of creating a positive corporate image to back up a shared sense of personal contribution to the security of Canada among all employees. But it would serve the goal of public information as well.

We particularly welcome the recent efforts of the Solicitor General to increase public awareness and understanding of the valuable work that CSIS does. Addressing the Confederation Club in Kitchener on April 21, 1988, for example, he revealed that as a result of information provided by CSIS more than a dozen foreign diplomats have gone home after their intelligence activities were uncovered and several more have been permanently expelled as *persona non grata*.* On May 5, 1988, in an address to the Kiwanis Club of Vancouver, he said CSIS carried out 50,000 security checks for the Calgary Olympics, and no terrorist slipped through the screening process. This too is information Canadians should have.

* After the end of the year under review, in June, 1988, a further example of such activity became public. We have had a preliminary briefing and, after further investigation, will comment in next year's annual report.

10. Five Years Later

In recent years, Parliament has provided, in some of the laws it passes, that they shall be reviewed within a set period of time. Section 69 of the *CSIS Act* is an example of this practice. It calls for "a comprehensive review of the provisions and operation of this Act" by a Parliamentary committee in 1989, five years after it came into effect.

In a democracy like ours, Parliament does not deliberate in a vacuum. Behind the debates of 1983 and 1984 lay the work of the McDonald Commission from 1977 to 1981 and a public discussion that can be traced back at least to the 1960s. As the Parliamentary spotlight turns on the *Act* again, the public has a voice. Experts will make their views known. So will others with a personal or professional interest in security intelligence. The media will report various views—and likely put forward some of their own.

We too plan to play a part. As close observers of CSIS since its creation, with full access to its files and an extra-bureaucratic standing that lets us speak out clearly within the limits imposed on us by considerations of national security, we feel a responsibility to share what we have learned. We have already made some suggestions in past annual reports. Looking ahead to 1989, we will have specific proposals for amendments in next year's annual report.

But Parliament and the public will not want to enter the review process cold. So, setting housekeeping matters aside for the moment, we set out in this chapter some of the issues that we see. We generally phrase them as questions because we do not want to seem to close any options.

Security Intelligence and Public Policy

The collection of information and its translation into intelligence is intended to serve Canada's long-term strategic and policy interests. This is only possible if there is constant communication between those who develop policy and those who produce intelligence. Many authors have commented—not specifically speaking of Canada, rather of a common pattern in the Western world—that the consumers of security intelligence often do not know what is available or what could be produced while, conversely, the producers of security intelligence often do not know the issues on which the policy-makers need intelligence.

In Canada, the users of intelligence are as numerous as the arms of the government. They include the Cabinet and senior officials of all departments and agencies. There are also many producers of many kinds of intelligence—economic, foreign, military and security (see Appendix C of this Report). CSIS is only one player.

Another issue arises out of the excellent relations that CSIS—fortunately—has with sister agencies in friendly countries. Since Canada's interests are similar to the interests of these countries, the intelligence that CSIS gets from them is mostly relevant to Canadian users. But CSIS must guard against adopting the outlook of these agencies at the expense of Canadian priorities.

In Chapter 6, we cite the Australian experience with an Office of National Assessment separate from the information gatherers in the intelligence agencies.

Should there be a new mechanism responsible for bringing intelligence of all kinds together before it is delivered to those who write policy and make decisions?

Security Intelligence and the Wider Community

A certain isolation from society as a whole is a fact of life for security intelligence services everywhere. For reasons of national security, an intelligence service cannot have frank exchanges with the private sector, politicians, educators, the news media—not even always with other arms of government.

Elsewhere in government the situation is quite different. Many officials have come to public service from successful careers in business, the professions, non-profit organizations, trade unions, the media and every other imaginable field. Specialized tasks are contracted out to experts. There is movement of personnel among departments and agencies. Public servants attend conferences where they exchange views and information with people in the private and voluntary sectors. In these and other ways, public servants remain integrated with society as a whole and have opportunities to keep abreast of developments in society.

Security intelligence officers, on the other hand, usually enter the field at an early age and stay with it until retirement. In Canada, CSIS officers are not covered by the *Public Service Employment Act*, so they are not "public servants" in strict legal terms. This means that rotation between CSIS and other arms of the federal government is, for all practical purposes, next to impossible. CSIS officers seek to guard their anonymity and stay away from places like conferences where the nature of their work might become obvious. For all of these reasons, CSIS forgoes many potentially fruitful exchanges.

Should the law be amended in such a way that the ability of staff to rotate between CSIS and other arms of the federal government is enhanced?

Would it be worth carrying out the extensive security clearances that would be required to allow outside experts to rotate through CSIS?

The Dissemination of Intelligence

The dissemination of intelligence under the control of CSIS is governed by section 19 of the *Act*, which does not contemplate disclosure outside government. We have already suggested (Annual Report 1985-86, page 45; Annual Report 1986-87, page 30), that there could be value in tipping individual Canadians when a voluntary organization they belong to is under, or risks coming under, clandestine foreign influence. It is not up to the Service to decide when members of the public should be told about foreign influence.

But it is not right that individual Canadians should, in all good faith, support and participate in the activities of foreign- influenced front groups whose covert objects are known to CSIS. Or that Canadian organizations with legitimate goals and methods should, in all good faith, become targets for infiltrators whose real aims as foreign agents are known to CSIS.

Should there be provision for some government body with authority to decide when CSIS should convey security intelligence to members of the public?

CSIS exchanges information with police and security agencies in Canada and abroad. We are told that care is taken to withhold intelligence from certain regimes that might make it a tool of oppression. However, CSIS has no comprehensive automated system for collating adverse personal information that it gives to police and other agencies. This is awkward for us, as we have an explicit duty under section 38 of the *Act* to monitor the provision of information to other agencies (see page 6).

Should there be an explicit requirement on CSIS to maintain statistical records of information passed to foreign agencies?

Threats to the Security of Canada

The cornerstone of CSIS's mandate is the definition of threats to the security of Canada, found in section 2 of the *Act*. Two expressions in that section need clarification:

- *Foreign influenced*: At the extreme, this is plain; there can be no doubt that a person who takes a hostile government's money under the table in return for pressing its views on the Canadian public is foreign influenced in a way that represents a threat to the security of Canada. But the *Act* surely does not contemplate the kind of foreign influence that colours the opinion and the talk of many, virtually all, Canadians—the subtle influence of foreign advertising, of foreign books, films and television, and so on.

- *Detrimental to the interests of Canada*: We have found uncertainty about the meaning of this term an issue in dealing with certain complaints. Is it "detrimental to the interests of Canada" simply to do things (a) without acknowledging publicly that one is (b) acting on behalf of a foreign power. Or is there a third specific condition—that (c) actual harm can be shown to be done. We have asked for an independent legal opinion on the meaning of this term.

Should the terms "foreign influenced" and "detrimental to the interests of Canada" be defined in the statute?

The Solicitor General has directed CSIS to use only non-intrusive techniques in its investigations under paragraph 2(*d*), which covers activities which have sometimes been referred to as "subversion". Any active investigation of these threats now requires the personal authorization of the Solicitor General. We have applauded these safeguards for lawful advocacy, protest and dissent (see Chapter 3, above). But they are only as strong as the commitment of the solicitor general of the day. What the present Solicitor General has ordered, a future solicitor general can rescind.

Should the requirement for special authorizations to investigate people involved in neither espionage nor terrorism be provided for in the statute?

Security Clearances

Section 42 of the *Act* provides for review (the new Government Security Policy uses the word "redress") where the deputy head of a department or agency denies federal employment to an individual or where a chance to sell goods or services to the federal government has been lost because an individual has been denied clearance.

But there are two situations in which an individual in the enterprise sector (whether public or private) has no access to effective review when an employment opportunity is denied because a clearance has been denied. One is where the individual is refused employment or is fired by a federal contractor to remove an obstacle to selling to the federal government.

The other is where no contract is involved. It is most easily explained with an example. Over the next few years, everyone with access to restricted areas in airports will require security clearance in which checks by CSIS play a key part. An airline pilot denied clearance will be unemployable. But no contract to supply goods or services to the federal government is involved. Rather, it is the airlines that use federal services. Yet the *Act* as now worded offers a pilot in this situation no effective review under section 42. The only avenues available would be a request for departmental reconsideration or an application to the courts.

We could hear certain aspects of such cases under section 41, which permits complaints "with respect to any act or thing done by the Service", but we do not consider this an adequate substitute for a section 42 complaint.

For one thing, section 41 adds a step to the process by requiring that a complaint first be addressed to the Director of CSIS. This is appropriate in most cases. Where CSIS has erred through inadvertance, say, it should have a chance to set the matter right on its own. But a recommendation to deny a security clearance is presumably a deliberate, careful decision that is not likely to be changed by the Director.

More important, there is no explicit provision in the *Act* for disclosure to the complainant under section 41. Generally speaking, this makes sense. In section 41 complaints, it is ordinarily the complainant who has the allegations and CSIS that puts up the defence. Security clearance complaints are different. As discussed in Chapter 7 above, we have a duty to advise complainants under section 42 of the allegations against them so they can make an informed response during our investigation. There are similar provisions for disclosure in citizenship and immigration cases.

> ***Should there be a more effective remedy where an individual is denied employment with a private firm because a security clearance has been refused on the advice of the Service?***

The *Act* provides a remedy through our complaints process when there is "denial of a security clearance" (section 42). The word "denial" can be narrowly interpreted to mean "refusal". That would open a loophole, because the authorities could effectively refuse a clearance without risking a complaint by letting the application sit indefinitely in the In basket, never formally rejecting it. We would likely take the position that "denial" should cover "unreasonable delay" as well as explicit refusal.

Should "denial" be defined in the statute to include unreasonable delay as well as explicit refusal?

CSIS Operations

We have previously (Annual Report 1986-87, page 12) suggested that there might be value in making provision for emergency warrants. Getting a warrant is currently a 16-stage process. An elaborate process is in order. Limiting the use of intrusive powers is one of the keys to the *CSIS Act*; it should not be too easy for CSIS to get a warrant.

But sooner or later an operation is bound to be compromised because a warrant could not be secured quickly enough. We have sketched the scenario in which CSIS learns at the eleventh hour that a terrorist is stopping over briefly in Canada. An instant warrant might be needed so meetings that the terrorist held during the stopover could be monitored electronically. This is the kind of occasion when the current procedure might prove too cumbersome. We continue to gather statistics on the length of time it takes to obtain warrants following normal procedures.

The Director could be authorized, with the agreement of the Solicitor General in each case, to issue short-term, non-renewable warrants that would remain in effect just long enough to permit an application to the Federal Court—up to 96 hours, say. We would envisage an early report to our Committee whenever an emergency warrant was issued.

Should the Director, with the agreement of the Solicitor General in each case, be authorized to issue short-term warrants in emergencies?

Controls on Warrants

Since the "mid-course correction" announced by the Solicitor General on November 30, 1987, the Service's Warrant Review Committee has included a "devil's advocate"—a lawyer, responsible to the Deputy Solicitor General, with a mandate to argue against each warrant application. This is one of a number of improvements in the process (see Chapter 3).

But our original proposal (Annual Report 1986-87, page 9), was that the devil's advocate should argue before the Solicitor General (whose personal approval is required before CSIS can formally apply for a warrant) or the Federal Court (which grants or refuses warrants).

Having given the matter more thought in the intervening year, we now think that the Federal Court is the appropriate forum for the devil's advocate. This seems to us the best substitute for the usual principle of natural justice—the requirement to hear both sides of an issue *(audi alteram partem)*. In security cases, the target obviously cannot be directly represented in court; it would defeat the purpose of a wiretap, say, if the target were warned through warrant proceedings.

Should statutory provision be made for a devil's advocate in warrant hearings? Should this official appear before the Federal Court?

Paragraph 21(4)(*f*) expressly gives judges of the Federal Court broad discretion to write conditions into warrants. In practice, there seem to be certain specific conditions that judges consider in each case. They ordinarily protect privileged solicitor-client communications, for example, by:

- Prohibiting the interception of communications at the office or residence of a solicitor or at any other place ordinarily used by a solicitor for the purpose of consulting clients. (This parallels the protection found in the *Criminal Code* for warrants issued to police.)
- Restricting the interception of calls between a target and the target's solicitor (or an employee of the solicitor) to those that the Director of CSIS or a regional director general determine are related to the threat to the security of Canada specified in the warrant.

We discussed this issue in some detail in our 1986-87 Annual Report (pages 19-20). The question we raised then remains.

> *Should explicit statutory protection be given to confidential solicitor-client communications in security intelligence investigations?* Behind that question lies a second: *Should the statute include a checklist of limitations that judges of the Federal Court must consider when they grant a warrant?*

Oversight

Under subsection 39(3) of the *Act*, the only information that CSIS can withhold from us is cabinet confidences. As we have already noted, only in Australia does an independent body like our Committee have such wide access to security intelligence files. The secrecy surrounding cabinet confidences has not been a problem in our day-to-day work.

However, it clearly limits the scope of the oversight we provide. We have no way of testing the Service's peformance against the demands that Cabinet has made on it. We have no way of knowing whether "problems" we identify flow directly from Cabinet orders.

Those of us who have been members of cabinets see no good reason for the lack of Committee access to relevant decisions of Cabinet or for insistence on cabinet secrecy in this case. The doctrine of cabinet secrecy is based on the need to let ministers disagree within the cabinet room, then present a united front when the debate is over. So the secrecy of cabinet discussion and the documents on which it is based is crucial to the principle of cabinet solidarity. But cabinet decisions must be revealed to those responsible for implementing them. Once a decision is made, it becomes known to public service employees. But not to us.

> *Should the Security Intelligence Review Committee have access to decisions of Cabinet relative to CSIS operations?*

Generally speaking, we rely on CSIS files for information. In the ordinary course of events, this is satisfactory. We have no reason to suspect CSIS of systematically trying to hide information from us. In an open society like ours, secrets have a way of surfacing eventually.

However, extraordinary circumstances could arise in which a member of CSIS felt it was necessary to bypass official channels to expose something believed to be wrong within the Service. We would hope that legitimate whistle-blowers would bring their stories to this Committee—in preference, especially, to telling them to the press. But the *Act* as written provides them no protection from discipline. In the United Kingdom, by contrast, a special official has been appointed to take "leaks" from members of the British Security Service ("MI-5") and investigate them. Members who provide information to this official are not required to identify themselves.

> *Should there be at least a statutory ban on prejudicial action against a member of the Service for conveying information to the Committee?*

Earlier in this Report (Chapter 3) we have said something of our protracted discussions with CSIS about the publication of warrant statistics. In this case we have come to a firm view:

> *Parliament should consider amending the statute so as to require the publication of specified warrant statistics.*

Access to Information and Privacy

We are not sure that the relationship between the *Access to Information Act* and the *Privacy Act*, on the one hand, and the *CSIS Act*, on the other, has yet been worked out with sufficient care. The Committee is, of course, aware of Parliament's report *Open and Shut* of March, 1987.

> *Should Parliament consider statutory amendments to reconcile access and privacy rights with the needs of national security?*

Basically Sound

Having raised all these matters, we should say that we believe the *Act* is basically sound. Most of the time and in most ways, it works well as a framework for carrying out the five basic principles articulated by the McDonald Commission:*

- The rule of law is paramount.
- The means of investigation must be proportionate to the gravity of the threat and the probability of its realization.
- The need for given investigative techniques must be weighed against the damage they might do to personal freedom and privacy or to valued social institutions.
- The more intrusive the technique, the higher the authority that must be required to approve its use.
- Except in emergencies, less intrusive techniques must be preferred to more intrusive techniques.

---

* *Freedom and Security under the Law*, the Second Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Ottawa, 1981), pages 513-514.

A civilian agency whose mandate is spelled out in law rather than by executive order, with clear political and judicial control and independent review, remains the appropriate model for security intelligence in Canada.

Appendix A

Ministerial Direction to CSIS, 1987-88

1. Procedures for Ministerial Consultation
2. Ministerial Prerogative
3. Disclosure of Certain Types of Information
4. Conduct of Activities Involving Certain Foreign Authorities
5. Ministerial Review of Administrative Arrangements
6. (Repetition of earlier ministerial direction)
7. Interim Management Instructions
8. Implementation of Government Policy
9. Disclosure of Information on Ministerial Authority
10. Clarification of Ministerial Policy
11. Disclosure of Information to Canadian Authorities
12. CSIS Audit Activities
13. Retention of Information
14. Ministerial Notice in Relation to Administrative Matters
15. Retention of Certain Types of Information and Review of Operational Matters
16. Transfer of CSIS Equipment
17. Delegation of Authority
18. CSIS File Disposal
19. (Repetition of earlier ministerial direction)

Appendix B

Summary Case Histories of Complaints Dealt With by the Security Intelligence Review Committee, 1987-88

Security Clearances

1. Alleged Subversion: A clearance was denied on the grounds of dishonesty because the individual failed to disclose full particulars of his past involvement in an organization regarded by CSIS as subversive, refused to give CSIS the names of others involved in this organization and, finally, allegedly falsified documents about his education and personal history.

The individual admitted during the Committee's investigation that he made a serious error in judgement when he misled CSIS in an interview about the extent of his involvement in the organization concerned. He explained that he "panicked". He also admitted that he was not completely frank in answering questions on a job application form; the information he provided was true, but it masked his involvement in the organization concerned. CSIS brought no evidence to support its allegation of falsification of documents.

The activities that gave rise to CSIS's concern about this individual had ceased five years before, and he had renounced his previous beliefs. The individual made mistakes, but his explanations were credible and his evidence before the Committee was open and honest.

CSIS and the employer also erred in this case. The Committee completely rejects the notion that refusal to name others has any place in a CSIS recommendation against granting a security clearance. The employer did not, as it should have under the Government Security Policy, give the individual a chance to respond to CSIS's allegations before the clearance was denied.

The Committee concluded that the complainant would be unlikely to act in a way that would pose a threat to the security of Canada and recommended that he be granted clearance.

Citizenship

2. Terrorism: Citizenship was denied a landed immigrant because of a belief that he would engage in activities defined by paragraph 2(*c*) of the *CSIS Act* as a threat to the security of Canada—namely, "activities within . . . Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within . . . a foreign state".

CSIS presented compelling evidence that this individual was active in a terrorist organization. He admitted to criminal offences for which he had been convicted in Canada. There was no dispute, for example, that he had helped load an illegal shipment of arms. He tried to convince the Committee that he had become involved in this organization without realizing what he was getting into. But his vagueness and frequent memory lapses damaged his credibility.

The Committee found that denial of Canadian citizenship was justified because there were reasonable grounds to believe that this individual would remain a security threat.

3. Objection Withdrawn: Citizenship was denied to a landed immigrant because of his membership in an organization considered subversive by CSIS. As a result of change in the treatment of alleged subversion, announced by the Solicitor General on November 30, 1987, the objection to citizenship for this individual was withdrawn. The Committee thereupon closed its file. This individual has since become a Canadian citizen.

4. Objection Withdrawn: Except that it involves a different individual, this case is identical with the previous one in every significant detail.

5. Objection Withdrawn: In this case, CSIS withdrew its objection before the Committee began its investigation, so no details of the allegations are on the file.

Immigration

6. Criminality: A deportation order was made against a landed immigrant on the basis of criminal intelligence reports indicating that he was involved in organized crime.

The RCMP presented strong evidence from a variety of sources demonstrating the complainant's involvement in extortion and threats on behalf of a criminal organization.

The complainant gave no oral evidence, although he was repeatedly urged to take advantage of his right to be heard. In a written submission he denied his involvement in organized criminal activity, but he did not deal in a substantial way with any of the RCMP's specific allegations. His counsel confined himself to challenging the Committee's jurisdiction and arguing that the Committee's procedures offended the *Canadian Charter of Rights and Freedoms*.

The Committee concluded that the deportation proceedings were justified.

7. Objection Withdrawn: An individual was denied entry to Canada because of RCMP allegations that he was involved in organized crime. But the RCMP withdrew its objection before the Committee began its investigation, so no details of the allegation are on the file.

Complaints under Section 41*

8. Alleged Harassment: An individual complained that there was no foundation to CSIS's suspicion that he had given Canadian secrets to a foreign government. He further complained that CSIS had investigated in a way that affected his physical and mental well-being as well as his professional reputation.

* In addition to the cases reviewed here, there were 30 complaints that were clearly out of the Committee's jurisdiction or in which the complainant offered no factual base on which an investigation could proceed. The complaints described here are those on which investigations were conducted and completed.

This individual had been seen taking money from a suspect official of the foreign government. The complainant, who was assisted by counsel, denied that he had betrayed Canadian secrets and he presented evidence to support his allegations of intrusive and illegal conduct by the Service.

The Committee concluded that CSIS had an obligation to carry out this investigation and that it had not made unreasonable or unnecessary use of its powers.

9. Payment of a Source: An individual who provided information to CSIS complained that he had not been paid as much as agreed upon. The dispute arose out of a misunderstanding. The Committee reviewed the situation and recommended a settlement. This recommendation was accepted by both parties.

Appendix C

The Intelligence Network in Canada

The Canadian Security Intelligence Service (CSIS) is part of a network of federal agencies concerned with security and intelligence. Except for the RCMP, it is the part best known to the general public; it is a key part; but it is, nonetheless, only a part.

This appendix briefly catalogues the major constituents of the network. It is based on a paper prepared in 1987 for members of the Security Intelligence Review Committee, to help them explore CSIS's mandate by placing it in the context of the work done by other agencies.* The Committee thought it would also be of interest to the public. Drastic trimming was required because much of the information in the original paper is secret. So the material presented here is by no means comprehensive. Much of it will be new to non-specialists, however.

The positions and agencies catalogued here are those that set priorities and that receive, produce, analyse and disseminate intelligence. By intelligence, we mean information in its finished form,** which provides a basis for government action. The protection of assets (referred to here as "security services") is touched on only incidentally.

It must be stressed that this catalogue is purely descriptive; no evaluation of the positions and agencies named can be read into it.

The Solicitor General

The Solicitor General is a central figure in the security intelligence network, responsible not only for CSIS but for the RCMP. He is assisted by the Deputy Solicitor General, by the Police and Security Branch within his Department and by the Inspector General.

With respect to CSIS, the Solicitor General has a number of responsibilities and powers under the *CSIS Act*. He issues written directions to CSIS on the conduct of both individual cases and entire classes of cases. His approval is required for each application CSIS makes to the Federal Court for a warrant to use such intrusive powers as wiretapping. His approval is also required for each agreement CSIS enters into with another agency—federal, provincial or foreign.

The Deputy Solicitor General assists and advises the Solicitor General. He coordinates the development of policy and is consulted extensively by the Director of CSIS. Under the direction of the Deputy Solicitor General, the Police and Security Branch initiates, develops and administers policies, operational directives and management systems on behalf of the Solicitor General. It also advises the Solicitor General on the activities of CSIS, the RCMP, federal and national law enforcement and counter-terrorism programs.

---

* The Committee acknowledges the generous assistance of many officials who provided information although they were under no obligation to do so.

** Analysts process raw information into intelligence by evaluating it for reliability and interpreting it to determine its meaning and significance. This is the stage in which processing (e.g., translation, photo interpretation, indexing) occurs as well as analysis.

You Get Letters . . . A Glossary of Acronymns

ARG — Assessment Review Group; an ARG is a task force that reviews material prepared by a SARG before it is submitted to IAC.

CCSI * — Cabinet Committee on Security and Intelligence.

CSE — Communications Security Establishment; Canada's signals intelligence agency.

CSIS — Canadian Security Intelligence Service.

EIC — Economic Intelligence Committee; an offshoot of IAC.

IAC — Intelligence Advisory Committee; with SAC, one of two principal subcommittees of ICSI; parent committee of EIC.

ICSI — Interdepartmental Committee on Security and Intelligence; a committee of deputy ministers that serves CCSI; its principal subcommittees are SAC and IAC.

IG * — Inspector General; the Solicitor General's watchdog on CSIS.

NSEU — National Security Enforcement Unit; units within the RCMP that, among other things, ensure liaison with CSIS and with other police forces.

PCO — Privy Council Office; as the Cabinet secretariat, the nerve centre of government operations in all fields, including security and intelligence.

RCMP — Royal Canadian Mounted Police.

SAC — Security Advisory Committee; with IAC, one of two principal subcommittees of ICSI.

SARG — Specialized Assessment and Review Group; SARGs are IAC task forces that produce foreign intelligence reports as well as longer research papers on specific topics.

SIRC — Security Intelligence Review Committee; Parliament's and the public's watchdog on CSIS.

TARC — Target Approval and Review Committee; an internal CSIS body that decides who should be investigated and how intensively.

* Rare; the full name is commonly used.

Canadian Security Intelligence Service (CSIS)

The core mandate of CSIS is spelled out in section 12 of the *CSIS Act*—to "collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada" and to "report to and advise the Government of Canada" on these matters.

CSIS's two major operational branches are Counter-terrorism and Counter-intelligence. An Analysis and Production Branch draws on information from the operational branches and from other covert and open sources to produce intelligence for use in many parts of the government. Another major program is security screening for public servants and others who have access to sensitive information and other assets vital to national security.

Important coordinating roles within CSIS are played by the Executive Committee, the Operations Policy Development Committee and the Target Approval and Review Committee (TARC).

Because much of CSIS's work must be done in secrecy, there are a number of controls on it. The role of the Solicitor General is discussed above. To use intrusive powers like wiretapping, CSIS requires warrants from the Federal Court of Canada. The *CSIS Act* also provides for monitoring by two external watchdogs—the Security Intelligence Review Committee and the Inspector General.

Inspector General

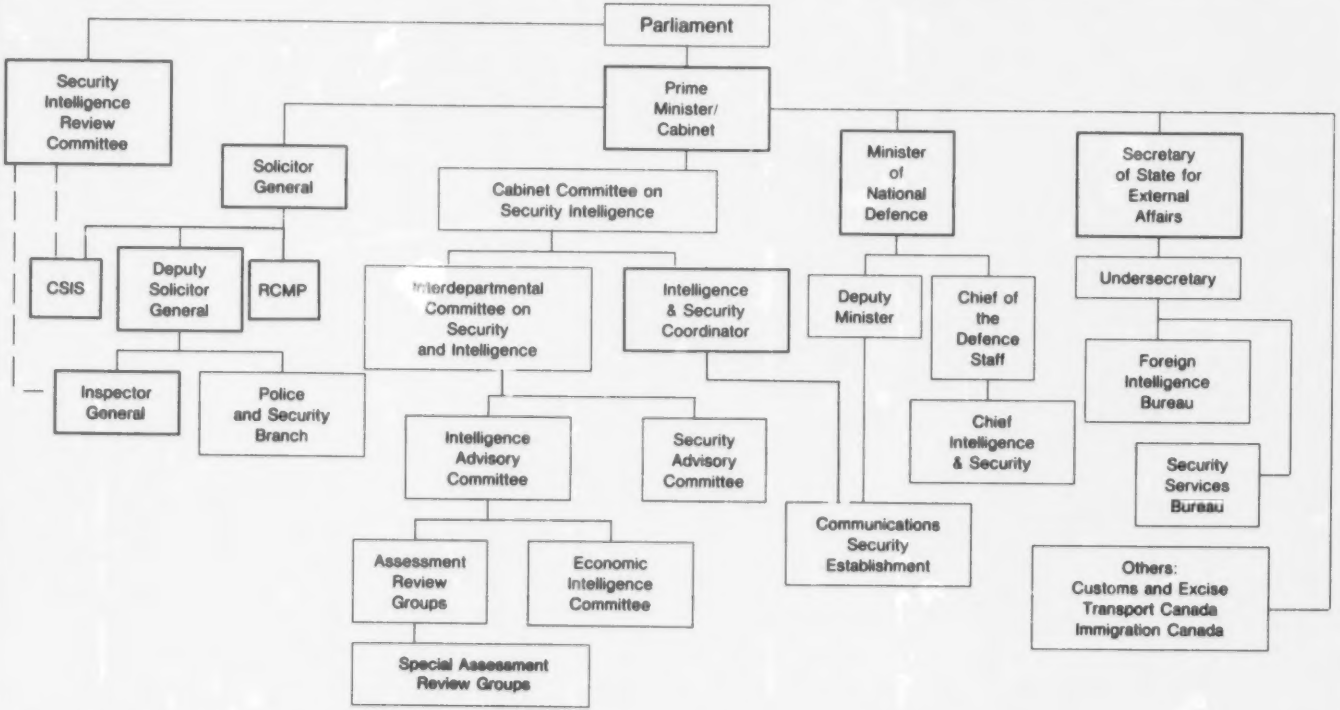
Reporting through the Deputy Solicitor General, the Inspector General is the Solicitor General's watchdog on CSIS, monitoring CSIS operations, policy, guidelines and internal controls. The Inspector General reviews the secret annual report that the Director of CSIS makes to the Solicitor General and issues a certificate stating (a) whether he is satisfied with this report, (b) whether the Service has remained within the bounds set by the *Act* and by the Solicitor General's instructions and (c) whether the Service has made "unreasonable or unnecessary" uses of its powers.

Security Intelligence Review Committee (SIRC)

SIRC is Parliament's and the public's eye on CSIS. It is composed of five part-time members appointed by the Governor in Council after consultations between the Prime Minister and the leaders of opposition parties recognized in the House of Commons.

The Committee has a dual mandate spelled out in the *CSIS Act*—oversight and complaints. In its oversight role, SIRC monitors CSIS's effectiveness with particular attention to ensuring that the Service does not make "unreasonable or unnecessary" use of its powers. SIRC also investigates complaints against CSIS and complaints about the denial of security clearances in public service employment, federal contracts, immigration and citizenship.

At a Glance . . . Major Components of the Intelligence Network



Notes: a) For simplicity's sake, only the most direct lines of authority are indicated.
b) Positions and departments with major statutory responsibilities are indicated by darker boxes.

SIRC's annual report is tabled in Parliament and is available to the public. Some of the special reports that SIRC makes to the Solicitor General on specific topics are also made public.

Royal Canadian Mounted Police (RCMP)

Part IV of the *CSIS Act* (the *Security Offences Act*) gives the RCMP primary responsibility for apprehending those who threaten the security of Canada or foreign diplomats in Canada. While CSIS pinpoints threats, the RCMP makes the arrests and assembles the evidence for the prosecution. The RCMP works closely with other police forces inside and outside Canada in carrying out this responsibility.

Through its National Security Enforcement Units (NSEUs), the RCMP exchanges information with CSIS and with other police forces on politically motivated crime, criminal activity by extremists, and other national security matters. NSEUs do not investigate specific offences but collect, coordinate and disseminate criminal intelligence. They are also responsible for issuing terrorist alerts and preparing threat assessments with regard to foreign diplomats in Canada and dignitaries from abroad visiting Canada.

The RCMP also provides a range of security related consultative and other protective services to senior officers of government, to foreign embassies and consulates, to dignitaries visiting Canada, at airports and elsewhere.

Transport Canada

The security of the national transportation system—on land and water and in the air—and its readiness to cope with emergencies is largely the responsibility of Transport Canada. The accent on airport security has risen in recent years because of frequent terrorist incidents in terminals and aboard aircraft in many parts of the world.

A Director General, Security and Emergency Planning oversees the work of four branches concerned with (a) policy and planning, (b) security operations, (c) intelligence, communications security and training and (d) emergency planning and the "Situation Centre" that would be the coordinator of operations in an emergency. The Director General is also responsible for the work of regional security directors.

Among other responsibilities, the Intelligence, Communications Security and Security Training Branch (a) coordinates the collection, analysis and dissemination of intelligence information from other agencies and (b) provides intelligence digests in support of departmental objectives as well as (c) providing threat assessments relevant to the protection of the national transportation system.

Employment and Immigration Canada

Immigration Canada's interests include (a) attempts by terrorists to use Canada as a haven, as a base of operations or for transit, (b) political and economic developments abroad that lead to international migration movements that could bring legal or illegal

immigrants to Canada and (c) immigration rackets, including the organized smuggling of people into Canada and the production, sale and use of fraudulent documents.

An Intelligence Division produces two kinds of intelligence, which it calls "strategic" and "tactical". Under the tactical heading, it develops and takes part in the development of programs for detecting fraudulent immigration practices—for example, distributing copies of newly-discovered forgeries to ports of entry so officals there will know what to look for. Strategic intelligence includes background briefing papers, immigration studies and trend analyses regarding enforcement/control activities and the development of recommendations for improving legislation, policy and procedures.

There is also a Security Review and Special Category Division whose work cannot be described here for security reasons.

Immigration Canada circulates an advisory notice to CSIS and other agencies on each application for a visa or for permanent residence in Canada, so they have an opportunity to raise any security concerns about the individual concerned.

Revenue Canada (Customs and Excise)

The security intelligence concerns of Customs and Excise are two-fold—"narco-terrorism" (drug trafficking aimed at raising money for terrorist operations) and illegal exports of defence and defence-related goods and technologies. Both these matters are dealt with by the Interdiction and Intelligence Division at headquarters and by Field Interdiction and Intelligence Units.

The headquarters Division gathers information on potential risks, the methods and routes used by offenders and other matters, and it produces both tactical intelligence for use in the field and strategic intelligence for senior management's use in planning. It liaises with the customs services of other countries, with law enforcement agencies in Canada and with such international agencies as the Customs Cooperation Council and Interpol.

Under the Export Control Program administered by this Division, export shipments are inspected to ensure that strategic goods and technologies are not being exported contrary to the *Export and Import Permits Act*.

Department of External Affairs

The Department has a Security Services Bureau whose responsibilities include developing and formulating policy for international cooperation against terrorism as well as providing a range of security services.

The Department of External Affairs has a Foreign Intelligence Bureau which collects and analyses information as a basis for providing intelligence to the Intelligence Advisory Committee (described below) as well as within the Department.

The Bureau has separate divisions for political and economic intelligence. Analysts are assigned on a regional basis (e.g., Middle East) or to global issues (e.g., nuclear proliferation). A third division interviews selected immigrants, defectors and Canadians who have lived in closed societies, to glean useful information not available from open sources. Such interviews are conducted only with the consent of the subject. The fourth division provides support for the rest of the Bureau.

Department of National Defence

The Chief, Intelligence and Security is responsible for the collection, production and dissemination of defence intelligence, including scientific and technical intelligence, for the Canadian Forces. A Director General, Intelligence and a Director General, Security report to the Chief. The Director General, Security is responsible for security services in the Department and the Forces.

Under the Director General, Intelligence are five directorates—(a) Defence Intelligence, (b) Current Intelligence, (c) Imagery Exploitation, (d) Scientific and Technical Intelligence and (e) Intelligence Plans and Doctrines. The Director General, Intelligence also maintains contact with intelligence agencies in other countries.

Communications Security Establishment (CSE)

CSE has a twin mandate—signals intelligence and the security of communications and data processing in federal agencies.

CSE provides a service of signals intelligence in support of Canada's foreign and defence policies based on the collection of foreign radio, radar and other electro-magnetic transmissions, and it distributes reports on what they reveal. It is responsible to the Minister of National Defence.

CSE's communications security role is to help federal agencies prevent unauthorized access to their telecommunications and electronic information processing. CSE also provides cryptographic key material and documentation to departments and agencies.

Coordinating Committees

There are a number of direct links, formal and informal, among the various security and intelligence agencies. In addition, a series of committees is in place to provide coordination.

Cabinet Committee on Security and Intelligence

At the centre of Canada's security intelligence network is the Cabinet Committee on Security and Intelligence. It is headed by the Prime Minister personally. Among its members

are ministers whose departments (a) make significant use of foreign and security intelligence, (b) are major gatherers or producers of intelligence or (c) are responsible for security operations. This Committee sets policy and determines the Government's security and intelligence priorities.

Privy Council Office (PCO)

In this as in other domains, the Prime Minister and Cabinet are supported by PCO, which includes a Security and Intelligence Secretariat headed by the Intelligence and Security Coordinator responsible for (a) interdepartmental coordination and (b) ensuring that the Prime Minister and the Cabinet Committee get the information and advice they need.

Interdepartmental Committee on Security and Intelligence (ICSI)

ICSI (pronounced "ick'-see") is headed by the Clerk of the Privy Council and includes deputy ministers of departments that are either major producers or major users of intelligence (or both), the Director of CSIS and the Commissioner of the RCMP.

Its responsibility is to develop proposals for the Cabinet Committee on Security and Intelligence. It has two principal subcommittees—the Security Advisory Committee (SAC) and the Intelligence Advisory Committee (IAC).

Security Advisory Committee (SAC)

SAC is concerned with security matters which affect federal government departments. The Committee, on which CSIS sits as a member, is chaired by the Deputy Solicitor General. SAC is supported by a small secretariat.

The Committee has a role in formulating security policy that has interdepartmental scope. It advises ICSI on security requirements and priorities. It carries out some of its functions through sub-committees which study specific issues, such as protection of information and property and counter-terrorism.

Intelligence Advisory Committee (IAC)

The IAC reflects the collective Canadian intelligence community. As such, the IAC members cooperate and coordinate the production of intelligence, drawing on research and analysis carried out by federal agencies, notably CSIS, the Department of External Affairs, the Department of National Defence and the Communications Security Establishment. Analysts meet in task forces called Special Assessment Review Groups (SARGs). Documents produced by SARGs are then reviewed by the Assessment Review Groups (ARGs) before being presented to IAC for final approval and dissemination.

The IAC chairman is the Intelligence and Security Coordinator in the Privy Council Office. CSIS is represented by the Director, with a designated alternate at the Deputy Director level.

An important subcommittee of IAC is the Economic Intelligence Committee (EIC), which directs the production of economic intelligence for IAC. CSIS is also represented on this subcommittee.

IAC also advises ICSI on policy issues such as intelligence needs and the coordination of intelligence programs and plans.

Appendix D

SIRC Staff on July 1, 1988

Maurice Archdeacon, Executive Secretary	990-6839
Danielle Blache, Senior Secretary	990-8442
Annie Demirjian, Executive Assistant	990-6319
Shirley Heafey, Senior Complaints Officer	993-4263
Arthur Graham, Director of Research	990-8051
Maurice M. Klein, Research Officer	990-8445
John M. Smith, Research Officer	991-9111
Joan Keane, Research Assistant	990-8443
Madeleine DeCarufel, Administration Officer and Registrar	990-8052
John Caron, Records Officer	990-6838
Roger MacDow, Records Clerk	998-5258
Diane Marion, Receptionist-Secretary	990-8441

COMITÉ DE SURVEILLANCE DES ACTIVITÉS
DE RENSEIGNEMENT DE SÉCURITÉ

Rapport annuel

1987-1988

Comité de surveillance des activités de renseignement de sécurité
365, avenue Laurier ouest
C.P. 2430, Succursale D
Ottawa (Ontario)
K1P 5W5

(613) 990-8441 — Les appels à frais virés sont acceptés et le standard téléphonique est ouvert de 7h30 à 18h00, heure d'Ottawa.

© Ministre des Approvisionnements et Services Canada 1988

N° de cat. JS 71-1/1988

ISBN 0-662-56247-X

Le 30 septembre 1988

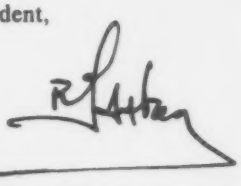
L'honorable James F. Kelleher, C.P., député, C.R.
Solliciteur général du Canada
Chambre des communes
Ottawa (Ontario)
K1A OA6

Monsieur le Ministre,

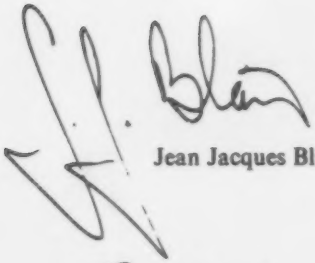
Conformément à l'article 53 de la *Loi sur le Service canadien du renseignement de sécurité*, nous soumettons au Parlement, par votre intermédiaire, le rapport annuel du Comité de surveillance des activités de renseignement de sécurité pour l'année financière 1987-1988.

Veuillez agréer, Monsieur le Ministre, l'expression de notre haute considération.

Le président,

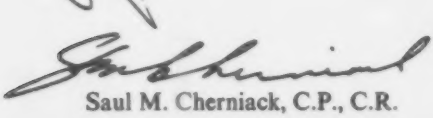


Ronald G. Atkey, C.P., C.R.



Jean Jacques Blais, C.P., C.R.

Frank McGee, C.P.



Saul M. Cherniack, C.P., C.R.

Paule Gauthier, C.P.

Franchir le cap

TABLE DES MATIÈRES

1. **Un second souffle** 1

Bons coups et mauvais points 1
Notre responsabilité 3
Ne pas faire comme si de rien n'était 3

2. **Contrôle** 5

Mandats judiciaires 5
Indications ministérielles 5
Ententes avec d'autres organismes 6
Divulgations dans l'intérêt public 8
Actes illégaux 8
Rapport annuel du SCRS et certificat de l'inspecteur général 8
Statistiques sur les activités opérationnelles 9
Études spéciales 9
Informations budgétaires 10
Consultations 10
Enquêtes et séances d'information 11
Nos relations avec le SCRS 12

3. **Opérations du SCRS** 15

Opérations d'antisubversion 15
Premier point de litige : les dossiers 16
Deuxième point de litige : le ciblage et les mandats judiciaires 17
Un exemple typique 19
Sources ouvertes 20
Statistiques sur les mandats judiciaires 21
Filtrage de sécurité 22

4. **Le SCRS lui-même** 25

L'Académie, hier et aujourd'hui 25
Représentation et bilinguisme 25
L'utilisation du polygraphe : de mal en quoi? 27
Gestion 29

5. **Opérations d'antiterrorisme** 31

Mandat du SCRS 31
Points et méthodes étudiés 31
Le défi 32
Priorité accrue 33
Ciblage et enquêtes 33
Politiques et pratiques 35
La production du renseignement 36
Conclusion 38

6. **De l'information au renseignement** 39

Le renseignement 40

Établissement des priorités 40
Sources et méthodes 41
Spécialisation 43
Satisfaction des besoins du client 44
Options éventuelles 45
Résumé 46

7. Plaintes 47

Les plaintes en 1987-1988 47
Qui décide? 48
Communication 49

8. Au CSARS 51

Notre travail de membres du CSARS 51
Rapport financier 51
Personnel 52

9. Besoin de savoir 53

Annuaires des services de renseignement et de sécurité 53
Liaison 53
Recherche académique canadienne 54
Médias : amis, adversaires ... ou les deux? 55
Porte-parole du SCRS? 56

10. Cinq ans après 57

Le renseignement de sécurité et la politique publique 57
Le renseignement de sécurité et la communauté canadienne 58
La communication de renseignements 58
Menaces envers la sécurité du Canada 59
Habilitations de sécurité 60
Activités du SCRS 61
Contrôle des mandats 62
Contrôle 63
Accès à l'information et protection des renseignements personnels 64
Fondamentalement bonne 64

Annexes

A Directives ministérielles 65
B Résumé des plaintes 67
C Le réseau de renseignement au Canada 71
D Personnel du Comité au 1er juillet 1988 83

1. Un second souffle

Nous espérons que nos successeurs pourront considérer l'année 1987-1988 comme celle où le Service canadien du renseignement de sécurité (SCRS) a franchi le cap.

C'est peut-être l'année où le SCRS a fait face aux événements les plus sombres de son histoire, particulièrement l'affaire du mandat judiciaire Atwal qui a entraîné la démission de son premier directeur (voir la page 12). Le secret étant essentiel à ses opérations, le SCRS ne peut pas avoir été heureux du nombre de profanes, qui ont franchis ses seuils. D'abord il y a eu le Groupe consultatif indépendant, armé des conclusions de notre dernier rapport annuel et de notre rapport spécial sur les langues officielles et les relations de travail, *Pour corriger une situation*, ainsi que d'un mandat ayant pour objet d'apporter des changements*. Ensuite, il y a eu un nouveau directeur provenant de l'extérieur du Service. La Direction de l'antisubversion a été dissoute et ses fonctions réassignées. Même si une partie du travail opérationnel s'est poursuivi normalement, personne ne peut blâmer les hommes et les femmes du SCRS de s'être parfois sentis frustrés.

Mais chaque chose a son bon côté. Le Groupe consultatif indépendant a élaboré une série de réformes réalistes fondées sur nos recommandations, et le gouvernement a commencé à les mettre en oeuvre. La disparition de la Direction de l'antisubversion empêchera toute réaction excessive aux menaces plutôt modestes que nos propres extrémistes constituent pour le Canada. Il semble à première vue que le nouveau directeur soit à la hauteur de la tâche.

En bref, nous croyons que cette année difficile a donné au SCRS l'occasion de reprendre souffle et de devenir enfin le genre d'organisme qu'envisageait le Parlement lorsqu'il a adopté la *Loi sur le SCRS* en 1984, c'est-à-dire un organisme civil aux priorités contemporaines qui concentrerait son attention sur la collecte et l'analyse de renseignements de sécurité dans le but de conseiller intelligement le gouvernement du jour.

Bons coups et mauvais points

Certaines des critiques qui se sont abattues sur le SCRS l'année passée étaient justifiées. En effet, la hâte ne peut excuser l'utilisation de renseignements de sources douteuses pour obtenir de la Cour fédérale l'autorisation de faire de l'écoute téléphonique dans l'affaire Atwal.

Mais le destin a voulu que la négligence du SCRS se retourne contre lui. À cause du mandat judiciaire défectueux, les procédures ont dû être suspendues contre cinq hommes accusés d'avoir comploté en vue d'assassiner un ministre du gouvernement de l'État du Punjab en Inde. Le SCRS a aussi été mis sur la sellette pour avoir négligé d'avertir la police à l'avance de la conspiration. Les conversations enregistrées dans l'affaire Atwal indiquaient

* Constitué le 22 juillet 1987 par le solliciteur général, le Groupe consultatif indépendant a présenté son rapport, *Des ressources humaines et un processus en transition*, qui contenait 34 recommandations, le 28 octobre 1987. Dirigé par Gordon Osbaldeston, ancien greffier du Conseil privé et actuellement agrégé supérieur de recherches à l'École d'administration publique de l'Université de Western Ontario, le groupe comprenait également Roger Tassé, ancien sous-solliciteur général et sous-ministre de la Justice qui pratique actuellement le droit à titre privé et Gérard Duclos, sous-contrôleur général, Direction de l'examen de la gestion, Conseil du Trésor.

clairement l'existence d'un plan pour assassiner le ministre, mais c'est seulement après l'attentat que le SCRS les a examinées.

Cet épisode a aussi contribué à créer une atmosphère de méfiance—pour ne pas dire de mépris—qui a suscité toutes sortes d'allégations au sujet de bêtises et d'irrégularités. Après avoir examiné les reportages des médias et suivi nos propres pistes, nous avons déterminé que la plupart de ces allégations étaient fausses. Voici nos conclusions :

- Le SCRS n'a *pas* commis de bévue dans l'entrée au Canada de Mahmoud Mohamed Issa Muhammad; une bévue a été commise, mais non par le SCRS.
- Le SCRS *n'a pas* non plus compromis la tentative de Muhammad de quitter le pays.
- *Rien* ne permet de croire jusqu'à présent que le SCRS avait des renseignements utiles et fiables qui auraient pu prévenir la tragédie d'Air India du 23 juin 1985, mois où un avion géant ayant quitté Toronto et Montréal pour Bombay s'est écrasé au large de l'Irlande faisant 329 morts; il était à prévoir qu'Air India pourrait être la cible d'un attentat, mais on ne peut vraiment pas dire que le SCRS ait obtenu un «tuyau» au sujet d'un incident précis.
- Il n'y a *non plus* aucune base à conclure que des données ont été perdues lorsque les bobines ont été effacées comme d'habitude après que les renseignements pertinents qu'elles contenaient eussent été notés.
- Le SCRS *ne cible pas* le mouvement ouvrier.
- Il *n'a pas* essayé de convaincre la *Sûreté du Québec* de favoriser un de ses informateurs lors de l'enquête sur des attentats à la bombe.
- Les plaintes de harcèlement qu'un homme d'Ottawa a adressées aux médias ainsi qu'à nous-mêmes *n'étaient pas* fondées; après étude, nous avons conclu que le SCRS avait mené des enquêtes raisonnables d'une façon professionnelle.

Le SCRS a eu aussi ses succès. Malheureusement, ils sont intangibles et caractérisés par l'absence d'événements plutôt que par leur présence. Et il faut être juste. N'oublions pas que la demande de renseignements de sécurité a été anormalement élevée en 1987-1988, année où le Canada a accueilli coup sur coup les sommets de la francophonie et du Commonwealth pour ensuite être hôte du monde à Calgary des 13 au 28 février à l'occasion des Jeux olympiques d'hiver. À la fin de l'année, le SCRS et la police préparaient en collaboration le Sommet économique de Toronto. Le fait que l'année s'est déroulée sans grave incident de sécurité est tout à l'honneur du dévouement et du professionnalisme des hommes et des femmes du SCRS.

Nous applaudissons à l'initiative du solliciteur général qui a lancé une série de conférences décrivant le travail du SCRS et expliquant assez longuement son importance pour les Canadiens. Pour des raisons de sécurité, le SCRS peut difficilement se vanter. Quant à nous, la loi nous impose une perspective de scepticisme raisonnée; il est donc juste que le solliciteur général comble toute lacune sur le plan des relations publiques.

Notre responsabilité

Pour notre part, nous estimons que le Parlement et le public s'attendent à ce que le Comité de surveillance des activités de renseignement de sécurité ait des opinions bien arrêtées et les énonce clairement dans ses rapports annuels et spéciaux.

Nous avons cherché à être juste, comme le montre notre rapport spécial sur ladite affaire Boivin*. Dans cette affaire, on avait allégué qu'un dirigeant syndical, Marc-André Boivin, qui était passible d'accusations liées à un attentat à la bombe, était un informateur du SCRS, et peut-être même un *agent provocateur*. Nous avons trouvé bien des choses que nous n'avons pas aimées dans l'enquête que nous avons effectuée à cet égard.

Nous avons appris, par exemple, que le SCRS avait conservé des renseignements que la GRC avait recueillis concernant des syndicats, et qu'il ne les avait pas encore examinés en relation avec les besoins de retentions strictement nécessaire de la *Loi*. De notre avis, cela allait à l'encontre de la *Loi sur le SCRS*. Nous avons aussi découvert avec consternation que le SCRS avait attendu deux jours avant d'avertir *la Sûreté du Québec* que, d'après ce que M. Boivin avait dit à son officier traitant du SCRS, il y avait lieu de croire que ces délits pénaux sérieux et spécifiques étaient sur le point d'être commis.

Mais nous avons conclu que le SCRS n'avait pas demandé à M. Boivin de faire rapport sur les activités de son syndicat et que celui-ci ne l'avait pas fait d'ailleurs, étant chargé des éléments «subversifs». Rien ne prouve non plus que le SCRS l'ait amené ni encouragé à influencer le syndicat ou à commettre des actes illégaux. Il n'était pas un *agent provocateur*. En ce qui concerne le ciblage et l'attribution des tâches, le SCRS était propre et nous l'avons dit.

Nous avons l'intention de continuer à remplir le mandat que nous avons reçu du Parlement et du public, c'est-à-dire de les informer des faits comme nous les voyons. Nous espérons que les changements qui surviennent dans la façon de procéder du SCRS nous donneront moins matière à critique.

Ne pas faire comme si de rien n'était

À vrai dire, le fil conducteur qui relie un grand nombre des problèmes que nous avons cernés est la tendance du Service à faire comme si de rien n'était. Nous ne disons pas qu'il défie délibérément et ouvertement la décision prise par le Parlement en 1984 de changer l'approche du renseignement de sécurité. Mais le SCRS semble souvent ne pas avoir la volonté de s'adapter.

Cela était peut-être inévitable dans les circonstances. Il semble clair avec le recul que les dérangements occasionnés par la séparation de la GRC ont été sous-estimés—même sur le plan matériel : quatre ans plus tard, le SCRS n'a toujours pas son propre quartier général,

* *Rapport présenté, aux termes de l'article 54, au solliciteur général du Canada sur l'usage par le SCRS de ses pouvoirs d'enquête en ce qui concerne le mouvement ouvrier*, rendu public par le solliciteur général le 29 mars 1988 (voir le chapitre 3 pour de plus amples détails sur nos constatations et nos conclusions).

par exemple des centaines de ses agents se rendent encore tous les matins à celui de la GRC à Ottawa, situé Promenade Alta Vista.

De toute façon, pendant les trois premières années, trop de personnes à tous les échelons ont invoqué—pour ne pas dire prétexté—la nécessité incontestée d'assurer la bonne marche des activités de renseignement de sécurité pour remettre certaines tâches à plus tard. Ainsi, le SCRS n'a pas encore fait concorder les dossiers dont il a hérités de la GRC avec les nouvelles exigences de la loi, ni commencer à établir un niveau acceptable de bilinguisme officiel, ni rechercher énergiquement des recrues ayant les antécédents requis en matière de recherche et de politiques d'orientations pour faire un travail moderne de renseignement de sécurité.

Si l'année 1987-1988 a été difficile pour le SCRS, elle l'a sûrement convaincu à jamais qu'il ne peut plus faire comme si de rien n'était. Nous avons choisi l'expression bien connue «franchir le cap» comme l'épigraphe de notre rapport annuel pour cette année. Les lecteurs constateront que nos critiques restent nombreuses, mais nous croyons que le SCRS est sur la bonne voie.

2. Surveillance

En vertu de la *Loi sur le SCRS*, le Comité de surveillance des activités de renseignement de sécurité (CSARS) est l'agent du Parlement et du public auprès du Service. Notre Comité est mandaté pour voir à ce que le SCRS effectue son travail efficacement, d'une part, mais sans empiéter d'une façon abusive ou inutile sur les droits individuels, de l'autre. Les tâches spécifiques que nous confère la *Loi* se divisent en deux grandes catégories : le surveillance et les plaintes. Une fois par an, il nous incombe également de faire un rapport sur notre travail. Il s'agit d notre rapport annuel où nous faisons une description de notre travail aussi complète que possible en restant toutefois dans les limites imposées par le besoin de protéger la sécurité nationale.

Le chapitre 8 du présent rapport porte sur le processus de traitement des plaintes. Dans le présent chapitre et les cinq qui suivent, nous faisons rapport de nos activités de contrôle en vertu des articles 38, 40 et 54 de la *Loi*. L'alinéa 38*a*) nous charge de «surveiller la façon dont le Service exerce ses fonctions» et il énumère une série de tâches spécifiques. L'alinéa 38*b*) et l'article 40 prévoient des recherches destinées à faire en sorte que «les activités du Service soient conduites conformément à la présente loi, à ses règlements et aux instructions du ministre ... et qu'elles ne donnent pas lieu à l'exercice par le Service de ses pouvoirs d'une façon abusive ou inutile». En vertu de l'article 54, nous pouvons présenter des rapports spéciaux au solliciteur général.

À cause de ses vastes pouvoirs d'enquête et du secret qui entoure inévitablement une grande partie de son travail, le SCRS est assujetti à un certain nombre de contrôles. Il peut exercer ses plus vastes pouvoirs comportant intrusion — l'interception du courrier et l'écoute téléphonique, par exemple — seulement s'il obtient un mandat judiciaire de la Cour fédérale du Canada. Chaque demande en ce sens exige l'approbation personnelle du solliciteur général. Ce dernier a également d'autres moyens de contrôle à sa disposition. Il approuve personnellement les ententes officielles que le SCRS signe avec les provinces afin d'avoir accès aux informations détenues par la police, et il donne des instructions officielles concernant la conduite d'affaires particulières ou d'entières classes d'affaires. Le solliciteur général a, en l'inspecteur général, son propre agent de surveillance du SCRS. Notre mandat s'étend à l'observation par le SCRS de tous ces contrôles.

Mandats judiciaires

Nous avons exprimé un certain nombre de préoccupations dans notre rapport annuel de l'an passé au sujet des processus liés au ciblage et aux mandats judiciaires. Par suite de la correction de trajectoire révélée par le solliciteur général le 30 novembre 1987, le SCRS a déjà fait beaucoup pour atténuer nos préoccupations. Les nouveaux arrangements sont examinés au chapitre 3 du présent rapport. Il reste à régler la question des relations privilégiées qui s'établissent entre un avocat et son client et celle des mandats d'urgence, lesquelles pourraient exiger des modifications de la *Loi*. Elles sont traitées au chapitre 10.

Indications ministérielles

Les directives ministérielles de 1987/1988 que nous avons reçues sont énumérées à l'annexe A du présent rapport. Après en avoir soigneusement examinées 13, nous sommes d'avis qu'elles ne permettent aucun exercice abusif ou inutile des pouvoirs du Service, ni

n'empiètent indûment sur les droits ou la vie privée des particuliers. En fait, la plupart tendent à circonscrire l'autorité indépendante du Service et à accroître son obligation de rendre des comptes au solliciteur général. Il en va de même pour les deux directives de 1986-1987 qui sont arrivées trop tard pour que nous puissions en traiter dans notre dernier rapport annuel. Également six directives de 1987-1988 sont arrivées trop tard pour être étudiées avant que ce rapport aille sous presse.

Comme nous l'avions promis (dans notre rapport annuel de 1986-1987 à la page 6), nous avons commencé à recueillir des statistiques sur les opérations pour lesquelles une approbation ministérielle est requise. Pour des raisons de sécurité, nous ne pouvons révéler les détails d'aucune de ces opérations, mais nous pouvons dire qu'elles ne sont pas tellement nombreuses.

En 1986-1987, nous avons découvert que nous ne recevions pas automatiquement copie de certains documents que nous considérerions comme des directives ou des instructions ministérielles (rapport annuel de 1986-1987, page 6), à cause de l'interprétation étroite qui était donnée au paragraphe 6(2) de la *Loi sur le SCRS*. Le Ministère du solliciteur général est en train d'établir des critères afin de s'assurer que nous recevrons tout ce qui tombe exactement sous le coup du paragraphe 6(2). Ce processus sera bientôt établi.

Toutefois, nous avons appris une bonne leçon cette année. Dans un communiqué de presse daté du 25 février 1988, le solliciteur général avait annoncé «de nouveaux contrôles ministériels sur les enquêtes du SCRS». (D'après ces contrôles, le SCRS doit obtenir l'autorisation personnelle du solliciteur général afin de mener toute enquête exigeant l'exercice de ses pouvoirs d'intrusion dans les affaires d'antisubversion.) Nous nous sommes aperçus que ces «nouveaux contrôles» n'avaient pas fait l'objet d'une communication formelle écrite au SCRS par le solliciteur général, ils avaient plutôt pris la forme de modifications du Manuel opérationnel du SCRS.

Le Manuel est un recueil de règles s'adressant point par point aux employés du SCRS. Le SCRS l'a rédigé, et il est sa responsabilité. Il comprend toutes les indications ministérielles, évidemment. Il donne de menus détails sur ces indications à bien des endroits, prescrivant les formules à utiliser et la voie hiérarchique à suivre.

Conformément au paragraphe 7(1) de la *Loi*, le SCRS consulte le sous-solliciteur général concernant les politiques opérationnelles générales. En fait, le sous-solliciteur général est consulté quand le Manuel est modifié. Nous attacherons dorénavant la même attention aux modifications du Manuel qu'aux indications ministérielles données en vertu du paragraphe 6(2) de la *Loi* étant donné qu'elles semblent, en pratique, avoir la même importance.

Ententes avec d'autres organismes

En 1987-1988, nous avons reçu copie de neuf nouvelles ententes du SCRS avec des organismes au Canada et d'une entente avec un organisme étranger. Nous sommes satisfaits de ces ententes pour ce qui est de leurs modalités, mais elles soulèvent deux questions.

La première question vise les arrangements entre le SCRS et les provinces en ce qui concerne l'échange d'informations avec les forces policières et l'assistance mutuelle. Trois des

neuf ententes internes signées l'année passée s'inscrivaient dans cette catégorie. Lorsqu'une entente a été conclue avec le Manitoba peu après la fin de l'année à l'étude, le SCRS avait des ententes avec toutes les provinces sauf une—le Québec. L'inexistence d'une entente officielle n'indique pas en soi une absence de collaboration susceptible de compromettre la sécurité nationale. Mais nous sommes d'avis que des ententes officielles sont utiles en ce qu'elles énoncent des lignes directrices à suivre et qu'elles permettent à chacun de connaître les actes qui sont permis et, ce qui est aussi important, ceux qui ne le sont pas.

L'autre question concerne le contrôle du tranfert des informations personnelles en la possession du Service. La plupart des ententes de ce dernier avec les ministères et organismes du gouvernement fédéral (lesquelles, soit dit en passant, constituaient les six autres ententes internes que nous avons vues l'an dernier) portent sur la prestation d'informations au SCRS en vertu de la *Loi sur la protection des renseignements personnels*. Nous n'avons rien à redire jusqu'ici.

Mais le système de gestion de l'information du SCRS ne permettait pas de savoir facilement quels renseignements et informations avaient été transmis à d'autres organismes, ce qui nous a effectivement empêchés—puisque nous ne pouvions pas faire des recherches manuelles qui auraient épuisé une armée de recherchistes—de remplir notre fonction statutaire en vertu du sous-alinéa 38*a*)(iii) de la *Loi sur le SCRS*, à savoir «surveiller les informations ou renseignements qui sont transmis en vertu de celles-ci [les ententes]» aux autres organismes, tant au pays qu'à l'étranger.

Empressons-nous d'ajouter que nos échantillonnages réguliers n'ont révélé aucun échange d'information que nous pourrions juger répréhensible; l'information fournie à d'autres organismes au sujet des résidents du Canada respectait les modalités des ententes pertinentes. L'information échangée en vertu de la plupart de ces ententes sert à la vérification des visas et à l'octroi des habilitations de sécurité.

Mais nous nous attendons à ce que la révision projetée du système informatisé de gestion de l'information du Service introduise un programme qui permettra d'obtenir facilement des données sur les échanges d'information au sujet de résidents canadiens qui ont eu lieu entre le SCRS et d'autres organismes (voir le Rapport annuel de 1986-1987, page 44). Le SCRS devra généralement être plus attentif en consignant ses activités, autant pour ses propres contrôles que pour les nôtres. Et nous désirons que soient élaborées une politique, une ligne directrice et une procédure de vérification spécifiques visant la divulgation de toute information sur des résidents canadiens.

En 1987-1988, le SCRS s'est acquitté d'une tâche que nous lui avions confiée (Rapport annuel de 1986-1987, page 21). Il a établi, à notre demande, un nouveau catalogue descriptif de ses arrangements avec les forces policières et les agences de sécurité dans les autres pays. Il s'agit d'une amélioration considérable par rapport à la liste incomplète que nous avons reçue en 1985. Après enquête sur la nature des ententes conclues avec 11 agences dans autant de pays, nous sommes convaincus que le SCRS a maintenant une liste à jour de ses arrangements internationaux.

Divulgations dans l'intérêt public

L'alinéa 19(2)*d*) de la *Loi* autorise la divulgation de certains renseignements aux fonctionnaires et aux ministres autres que le solliciteur général, le secrétaire d'État aux Affaires extérieures et le ministre de la Défense nationale. Le paragraphe 19(3) exige que le directeur nous fasse rapport de ces divulgations. Aucun rapport n'a été fait en 1987-1988.

À cet égard, nous nous étions déjà dits préoccupés (rapport annuel de 1986-1987, page 34) par le fait que la *Loi* n'indique pas que les Canadiens individuels doivent être mis en garde lorsqu'ils sont emportés dans l'orbite d'organismes de façade servant en secret des buts ou des gouvernements étrangers susceptibles de menacer la sécurité nationale du Canada. Si nous ne nous étendons pas sur ce sujet ici, c'est seulement parce qu'il est traité cette année au chapitre 10, où nous jetons déjà un regard sur l'examen quinquennal de la *Loi*.

Actes illégaux

Nous avons reçu deux rapports en vertu de l'article 20 de la *Loi*. Cet article exige que le directeur du SCRS prévienne le solliciteur général lorsqu'il semble qu'un employé peut avoir commis des actes illicites dans l'exercice de ses fonctions. Nous recevons copie de tout rapport que le solliciteur général peut transmettre au procureur général du Canada en ce sens, ainsi que de toute observation qu'il peut formuler. Dans le premier cas, aucune accusation n'a été portée. Dans le deuxième, le procureur général a renvoyé l'affaire aux autorités provinciales qui n'avaient pas décidé à la fin de l'année s'il convenait ou non de porter des accusations. Dans les deux cas, nous sommes convaincus que la direction du SCRS a pris des mesures sévères en vue de protéger le public contre tout acte illégal qui pourrait être commis sous le couvert de la *Loi sur le SCRS*.

Rapport annuel du SCRS et certificat de l'inspecteur général

L'article 33 de la *Loi sur le SCRS* prévoit que le directeur du SCRS doit présenter un rapport annuel au solliciteur général et que l'inspecteur général doit remettre un certificat où il indique si le rapport est acceptable—en particulier si le Service a accompli des actes qui ne sont pas autorisés dans la *Loi* ou qui contreviennent aux indications données par le solliciteur général, ou encore s'il a exercé ses pouvoirs d'une façon abusive ou inutile. L'article 33 indique également que le rapport annuel du directeur et le certificat de l'inspecteur général doivent nous être transmis.

Nous sommes incapables dans le présent rapport de commenter le certificat de l'inspecteur général pour 1987, étant donné qu'il n'y avait pas d'inspecteur général pour en présenter un à ce moment-là. M. Richard Gosse, qui a rempli cette charge avec distinction depuis sa création en 1984, a quitté son poste en février pour devenir le premier président de la Commission des plaintes du public pour la GRC, et il n'avait pas été remplacé à la fin de l'année budgétaire. Nous saisissons cette occasion pour remercier M. Gosse d'avoir collaboré avec nous. Nous avons constaté que nous pouvions compter sur son personnel qui était consciencieux et minutieux dans les recherches qu'il a effectué pour notre compte en vertu de l'article 40 de la *Loi*. Le successeur de M. Gosse aura tout un exemple à suivre.

Statistiques sur les activités opérationnelles

Le sous-alinéa 38*a*)(viii) de la *Loi* nous autorise explicitement à «réunir et analyser des statistiques sur les activités opérationnelles du Service». Nous continuons de réunir et d'analyser des statistiques dans un certain nombre de domaines—l'utilisation des techniques d'enquête comportant intrusion (par exemple le nombre d'écoutes téléphoniques autorisées par voie de mandat judiciaire), la circulation et la conservation des données (par exemple la conservation des dossiers; voir la page 16), [illegible] veaux d'enquête (par exemple le nombre d'enquêtes sur le terrain menées dans le cadre des filtrages de sécurité; voir la page 22).

Le SCRS nous rencontre à l'étape de la rédaction pour discuter des huit à dix documents statistiques que nous rédigeons chaque année. De cette façon, nous arrivons à nos interprétations de ces statistiques avec une connaissance approfondie de celles du SCRS, et ces réunions nous apportent beaucoup.

Études spéciales

Nous avons présenté deux rapports spéciaux au solliciteur général en vertu de l'article 54 de la *Loi* en 1987-1988. Le premier portait sur l'usage par le SCRS de ses pouvoirs d'enquête en ce qui concerne le mouvement ouvrier. Comme nous l'avons mentionné au chapitre 1, ce rapport a été rendu public par le solliciteur général le 29 mars 1988. Nous présentons certaines de nos conclusions au chapitre 3.

L'autre rapport portait sur le filtrage de sécurité en matière d'immigration. Il n'a pas été rendu public parce qu'il contient des informations qui risquent de compromettre la sécurité nationale. Le rapport suscite bien des préoccupations importantes, et il sert à une étude interministérielle effectuée par suite des recommandations que le Comité permanent de la Chambre des communes chargé du travail, de l'emploi et de l'immigration a présentées dans son rapport du 17 juin 1986.

Également, tel qu'annoncé l'an passé, nous avons commencé à examiner le régime de protection des avoirs techniques et scientifiques au Canada, à partir principalement d'entrevues structurées avec des représentants fédéraux qui oeuvrent dans ce domaine. Nous avons rencontré des personnes du bureau du Conseil privé, de Revenu Canada (Douanes), du ministère des Affaires extérieures, du ministère de la Défense nationale, Approvisionnements et Services Canada et la GRC, ainsi que des représentants du SCRS. Vu le nombre importants de joueurs dans ce domaine, les analyses et les consultations aboutissants au rapport final, ne sont pas encore prêtes.

Nous poursuivons un programme d'études qui nous permettra d'examiner à fond les fonctions de base du Service avant l'expiration de notre mandat en 1989. En 1986-1987, nous avons étudié le programme d'antisubversion, qui soulevait de graves questions concernant le «ciblage»—c'est-à-dire la façon dont le SCRS choisit les personnes sur lesquelles il enquêtera (voir le chapitre 3 du présent rapport pour une mise à jour). Cette année nous nous sommes concentrés sur le programme d'antiterrorisme (voir le chapitre 5) et l'évaluation des renseignements (chapitre 6). Dans l'année qui viendra, nous nous tournerons vers le programme de contre-espionnage et sur les enquêtes du SCRS, s'il y en a, sur le mouvement pour la paix au Canada.

En effectuant ces grandes études, nous avons pris l'habitude d'élaborer un mandat détaillé avec les gestionnaires responsables du SCRS. Cela leur permet de comprendre pleinement les informations dont nous avons besoin et de nous indiquer les dossiers et documents qui pourraient nous intéresser. Le Service, pour sa part, désigne habituellement un membre de la section à l'étude à titre d'agent de liaison. Cet agent travaille avec nous afin que l'étude soit gérée de façon à nuire le moins possible aux responsabilités opérationnelles du SCRS.

Informations budgétaires

Nous recevons la mise à jour du Plan opérationnel pluriannuel (POP) que le SCRS, comme tous les organismes du gouvernement fédéral, dresse annuellement. Nous reconnaissons que les informations figurant dans la mise à jour du Service pour 1987 remplissent les exigences du Conseil du Trésor. Mais elles ne donnent pas à elles seules l'aperçu que nous voulons avoir du SCRS en tant qu'organisme. En particulier, elles ne nous permettent pas de répondre à la question : «Le SCRS a-t-il l'argent et le personnel dont il a besoin?»

Il faut préciser que les informations accessibles ne montrent pas que le SCRS bénéficie d'un excédent de fonds ou de personnel. C'est plutôt le contraire qui est vrai : malgré un budget qui monte en flèche, nous avons l'impression qu'on lui demande d'en faire un peu trop avec les ressources dont il dispose.

Mais nous avons maintenant demandé au Service de nous fournir des informations détaillées sur ses ressources financières et humaines, et particulièrement un rapprochement des données du POP avec celles qui se trouvent dans le Budget des dépenses principales, des états financiers vérifiés de fin d'année comme ceux que d'autres organismes insèrent dans les Comptes publics du Canada, et des renseignements précis sur la répartition des années-personnes entre les diverses fonctions. Nous espérons effectuer un examen des ressources du SCRS et de la façon dont il les utilise avant la fin de notre mandat.

Consultations

En remplissant notre rôle lié au contrôle, nous tenons également des dizaines de consultations d'usage. Nous avons des réunions de groupe avec le solliciteur général tous les trois mois, et notre président le rencontre mensuellement. Il tient également des réunions occasionnelles avec le sous-solliciteur général et il rencontre régulièrement le directeur du SCRS. Le Comité plénier et le président rencontrent tous deux l'inspecteur général à l'occasion, et il y a des réunions fréquentes entre ce dernier et notre secrétaire exécutif. L'an dernier, des réunions ont également eu lieu avec le Groupe consultatif indépendant constitué par le solliciteur général en réponse à des préoccupations que nous avions exprimées dans des rapports précédents.

En 1987-1988, nous avons continué à visiter les bureaux régionaux et de district du Service plutôt que de limiter nos contacts au quartier général à Ottawa. Cela nous permet d'être renseignés sur les opérations régionales par les gens qui sont le plus au courant. Nous avons habituellement avec les gestionnaires des régions ou des districts et avec le ban et l'arrière-ban des réunions séparées au cours desquelles nous discutons franchement des préoccupations des employés sur le terrain et répondons à des questions au sujet de notre

propre rôle. Le SCRS a été très coopératif dans le cadre de ce programme. Pendant l'année à l'étude, nous avons visité quatre bureaux régionaux et de district, soit ceux de Winnipeg, de Vancouver, de Montréal et de Toronto. Pendant l'année qui viendra, nous visiterons les bureaux de Halifax et de Québec, et nous retournerons à Vancouver et à Toronto.

Pour élargir nos horizons, nous avons visité Hong-kong, l'Australie et la Nouvelle-Zélande en novembre 1987. À Hong-kong, où les demandes d'immigration entrent à flots, nous nous sommes arrêtés au travail qui s'y fait. Environ 25 000 demandes d'immigration sont présentées à Hong-kong chaque année et ce nombre va croissant à mesure que les habitants et les capitaux recherchent des abris en prévision de 1997, année où la Chine assumera la responsabilité administrative de Hong-kong. Ce que nous avons appris là-bas nous a matériellement aidé à rédiger notre rapport spécial sur le filtrage de sécurité en matière d'immigration.

Les cas de l'Australie et de la Nouvelle-Zélande étaient particulièrement intéressants étant donné que ce sont deux pays avec lesquels le Canada entretient d'excellentes relations. De plus, le processus de traitement des plaintes de l'Australie est plus semblable au nôtre que celui de tout autre pays. Nous nous fondons sur des informations que nous avons obtenues là-bas pour formuler certaines observations qui figurent dans le présent rapport.

Enquêtes et séances d'information

À l'exception seulement des documents confidentiels du Cabinet, nous avons accès à toutes les informations en la possession du SCRS. L'an dernier, nous avons présenté 95 demandes écrites au Service et nous avions reçu 85 réponses à la fin de l'année. À ce moment là il restait donc un total de 10 questions sans réponse; la plupart d'entre elles auraient été posées au Service dans le dernier mois de l'année financière. Comme le prévoit la *Loi sur le SCRS*, nous demandons parfois au Bureau de l'inspecteur général d'effectuer des recherches pour nous. En 1987-1988, ce bureau avait réalisé à notre intention trois examens portant sur des activités spécifiques du Service.

Le SCRS nous donne également des séances d'information sur des questions particulières. Par exemple, en 1987-1988, il nous a fourni des rapports d'étape mensuels concernant l'enquête sur le désastre d'Air India et l'explosion à l'aéroport de Narita, questions qui ont gravement préoccupé le public. Nous avons déjà, au chapitre 1, traité de certaines allégations qui ont été faites par les médias. En ce qui concerne les bobines effacées, le Service aurait gravement tort de laisser les enregistrements téléphoniques s'accumuler indéfiniment au cas où ils contiendraient des renseignements qui pourraient éventuellement être utiles à la police. Le rôle du SCRS est de recueillir des *renseignements de sécurité*. Les enregistrements téléphoniques contiennent habituellement un grand nombre d'informations personnelles et autres qui n'ont pas leur place dans des dossiers secrets. Nous croyons que le SCRS a raison de détruire les bobines après avoir noté les informations pertinentes qu'elles renferment.

Qui plus est, ce n'est pas à nous de donner au public des renseignements supplémentaires sur la tragédie d'Air India. Nous sommes profondément conscients du fait que les Canadiens se sentent frustrés parce que, trois ans plus tard, des accusations n'ont pas encore été

portées.* La GRC poursuit son enquête, et le rôle du SCRS à l'heure actuelle consiste à fournir à la Gendarmerie une aide en matière de renseignements de sécurité. Nous continuons de surveiller la situation de près.

Nous avons également bénéficié de séances d'information sur «l'affaire du mandat judiciaire Atwal». Les procédures de la Cour fédérale du Canada ont mis les grandes lignes de cette affaire dans le domaine public. Ce qui n'est peut-être pas bien compris c'est que le Service n'a pas délibérément «cuisiné» sa demande de mandat judiciaire en incluant des informations d'une source non digne de foi. Lorsque l'affidavit a été rédigé, l'information était considérée comme fiable. C'est seulement après que les documents eurent été reçus au quartier général du SCRS que le bureau régional concerné a décidé que la source n'était pas digne de confiance. Il a manqué à son devoir en ne prévenant pas le quartier général. Il s'agit là d'une faute grave, mais non d'un acte de falsification délibérée. Nous croyons que les nouvelles procédures décrites au chapitre 3 constituent une protection supplémentaire contre ce genre d'omission.

Dans une autre affaire qui est venue à la connaissance du public pendant l'année, nous avons conclu que le SCRS avait bien agi vis-à-vis de Ryszard Paszkowski qui, en janvier 1988, était allé raconter aux médias une longue histoire selon laquelle son travail pour le SCRS lui aurait fait faire un an de prison pour piraterie d'avion en Allemagne de l'Ouest. Comme le solliciteur général l'a confirmé à la Chambre des communes**, Paszkowski a travaillé pour le SCRS après être entré au Canada illégalement, mais le SCRS ne l'a pas amené au pays pour être un agent double, comme l'affirme le plaignant, et il a mis fin à ses rapports avec lui avant que Paszkowski quitte le Canada volontairement en août 1986 pour se rendre en Italie, d'où il a été extradé par l'Allemagne de l'Ouest.

Nos relations avec le SCRS

Nous continuons d'entretenir des relations à distance avec le SCRS. Cela est dans l'ordre. Nous et le Service avons finalement le même objectif, à savoir des opérations efficaces de renseignement de sécurité dans les limites imposées par les valeurs d'une société libre et démocratique. Mais nos rôles sont différents et, dans la mesure où nous faisons tous deux notre travail, ils créent inévitablement des conflits occasionnels entre nous.

En général, nous croyons que le SCRS joue franc jeu dans ses rapports avec nous. Dans le domaine du contrôle, nos relations sont pour le moins correctes. Elles sont souvent cordiales. Nous avons déjà noté dans le présent chapitre que le SCRS s'est montré très coopératif en organisant nos visites de ses bureaux régionaux et qu'il ne nous a pas empêchés de tenir des réunions distinctes avec le ban et l'arrière-ban et avec les gestionnaires régionaux.

* Dans le cas de l'explosion à l'aéroport de Narita, les poursuites judiciaires sont entamées. La police Britannique a arrêté un suspect en Angleterre le 5 février 1988. Le 9 août 1988, à Londres, le juge a ordonné l'extradition de Anderjit Singh Reyat au Canada pour faire face à des accusations dont deux accusations d'homicide involontaire pour les morts à Narita. Au moment où nous mettons sous presse, l'accusé a soumis un appel de cette ordonnance.

** Canada, débats de la Chambre des communes, le 22 janvier 1988.

Lorsque nous enquêtons sur des plaintes spécifiques, les relations entre nous sont plus distantes et formelles. Cela est aussi dans l'ordre. Nous agissons à titre d'organisme quasi judiciaire.

Nous comprenons fort bien que le Service fasse preuve d'une certaine prudence; quoique nous rejettions toute suggestion à l'effet que nos pouvoirs de surveillance et d'enquête sont néfastes au Service. De plus en plus, toutes les agences de renseignement de sécurité des pays de l'Ouest sont sujettes à une forme quelconque de contrôle, mais l'Australie, à notre connaissance, est le seul autre pays où un organisme indépendant* a un accès illimité aux dossiers du renseignement de sécurité.

Nous aimons à penser que nos relations avec le Service sont empreintes de tension créative. Même si nous critiquons souvent les systèmes dans nos rapports—cela est dû à la nature de notre mandat—nous désirons exprimer encore une fois notre respect et notre admiration pour les employés du Service. Ils ont un rôle difficile à jouer en ce sens que, comme on l'a souvent fait remarquer, leurs succès doivent demeurer dans l'ombre alors que leurs échecs inévitables semblent toujours émerger au grand jour.

* L'inspecteur général

3. Opérations du SCRS

L'essence du mandat du SCRS est exposé à l'article 12 de la *Loi sur le SCRS*. Cet article affirme que le SCRS «recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard».

Les «menaces envers la sécurité du Canada» sont définies à l'article 2. Elles se divisent en quatre catégories : l'espionnage ou le sabotage, l'intervention étrangère clandestine dans les affaires canadiennes, l'utilisation de la violence pour atteindre des objectifs politiques au Canada ou dans un autre pays et, enfin, les tentatives cachées ou éventuellement violentes pour renverser notre régime de gouvernement constitutionnellement établi. «Les activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord» sont explicitement exclues à moins d'être liées à l'une des menaces énoncées à l'article 2.

Au chapitre 2, nous avons traité des contrôles qui sont exercés sur l'utilisation par le Service de ses pouvoirs dans l'exécution de son mandat. Le présent chapitre et les trois qui suivent examinent les questions opérationnelles—comment le SCRS garde la sécurité du Canada.

Opérations d'antisubversion

Comme nous l'avions recommandé dans notre dernier rapport annuel (page 45), la Direction de l'antisubversion du SCRS a été dissoute en novembre 1987 et ses responsabilités ont été réassignées. En conséquence, les enquêtes que le SCRS tient maintenant sur les ressortissants canadiens sont plus conformes aux menaces limitées que ces derniers peuvent constituer envers la sécurité nationale. De même, ces enquêtes respectent davantage la limite du «strictement nécessaire» prescrite à l'article 12. Les cas d'activités étrangères soupçonnées d'être contraires aux intérêts du Canada sont maintenant traités par la Direction du contre-espionnage, et ceux qui semblent poser un risque de violence réel sont traités par la Direction de l'antiterrorisme.

Ce qui reste des cibles d'antisubversion est maintenant contrôlé par la Direction de l'analyse et de la production, qui verse aux dossiers toutes les informations pertinentes qu'elle tient des médias ou à la suite d'autres enquêtes afin de fournir au gouvernement ce que le solliciteur général a nommé «un rapport de surveillance*». Mais le Manuel des opérations a été modifié de façon à ce que le solliciteur général soit tenu d'autoriser personnellement toute enquête active qui sera ouverte sur ces affaires. Nous croyons qu'il s'agit là d'un bon moyen de contrôle; c'est toujours le SCRS qui décide d'ouvrir une enquête, en dehors de toute considération politique partisane, mais quelqu'un est responsable à l'échelon politique lorsqu'une telle initiative est prise.

---

* Solliciteur général du Canada, Notes en vue d'une allocution au cours de la conférence sur la défense d'une cause, la protestation et la manifestation d'un désaccord, Université Queen's, le 25 février 1988.

Au total, un peu plus de 3 000 dossiers qui étaient activement à l'étude dans le cadre du programme d'antisubversion restent ouverts. Mais il n'y en reste plus qu'un petit pourcentage sur lesquels les directions de l'antiterrorisme ou du contre-espionnage enquêtent activement. Le SCRS ne fait que surveiller les autres.

Après avoir examiné le ciblage et l'exercice des pouvoirs comportant intrusion, nous pouvons affirmer que, entre le moment où le solliciteur général a fait son annonce et la fin de l'année, aucun groupe n'a fait l'objet d'une enquête seulement en vertu de l'alinéa 2*d*) de la *Loi*—la disposition sur «l'antisubversion».

Premier suivi : les dossiers

La controverse entourant le sort du programme d'antisubversion a mis en lumière bien des informations factuelles qui n'étaient pas accessibles auparavant sur la mesure où le Service accumule des renseignements sur des Canadiens particuliers. Dans notre dernier rapport annuel (page 43), nous avons dit que la Direction de l'antisubversion «a probablement plus de 30 000 dossiers, au bas mot, sur des particuliers». Nous savons maintenant que ce chiffre péchait par défaut comme nous nous y attendions. Le Service a subséquemment fait la recherche nécessaire et découvert environ 54 000 de ces dossiers.

Dans le même passage, nous avons dit que des enquêtes actives avaient été entreprises sur un petit pourcentage seulement de particuliers sur lesquels la Direction de l'antisubversion avait ouvert un dossier. Nous n'avons pas révélé combien de personnes exactement étaient touchées parce que ce renseignement était classifié, mais le SCRS a subséquemment informé les médias qu'il s'agissait de 3 867 personnes.

La grande majorité des dossiers d'antisubversion déjà inactifs il y a un an, dont tous ceux qui concernent les syndicats, sont actuellement sous clé en attendant d'être examinés. Maintenant que le moratoire sur la destruction des dossiers, qui était en vigueur dans l'ensemble du gouvernement a été levé, un grand nombre de ces dossiers devraient bientôt prendre le chemin de la déchiqueteuse, d'autres celui de la collection fermée des Archives publiques du Canada.

Nous nous sommes également dits préoccupés, dans notre rapport annuel de l'année dernière (pages 25 à 28), par l'information dont le SCRS avait héritée du Service de sécurité de la GRC, y compris celle qui figure dans la plupart des dossiers d'antisubversion. Nous croyions qu'une grande partie de ces informations ne répondaient pas au critère du «strictement nécessaire» et ne correspondaient pas à la définition d'une «menace envers la sécurité du Canada» donnée à l'article 2. De plus, nous avons noté que, à cause du moratoire, des dizaines de milliers de dossiers qui n'étaient plus utiles existaient toujours.

Nous ne nous opposons pas au moratoire lui-même. Il a été imposé en février 1985, après que la Commission royale d'enquête sur les criminels de guerre (Deschênes) eût découvert que des dossiers d'immigration dont elle avait besoin avaient été systématiquement détruits des années auparavant. De toute façon, maintenant que le moratoire a été levé, une section du SCRS a été constituée et chargée d'examiner les dossiers et de désigner ceux qui doivent être détruits. Quelque 67 000 dossiers que la GRC comptait détruire

avant la création du SCRS l'ont déjà été. Nous continuerons de surveiller l'état d'avancement de ce travail.

Quant aux dossiers actifs contenant des informations qui avaient été recueillies par la GRC et qui ne satisfont peut-être pas les critères des articles 2 et 12, le SCRS a déjà commencé à les examiner en vue de radier l'information qu'ils ne devraient pas contenir. Nous reconnaissons qu'il faudra des années pour dépouiller tous les dossiers, et nous suivrons également l'état d'avancement de cet exercice.

De plus, à compter de janvier 1988, aucune information ne peut être versée à ces dossiers à moins que les sujets ne tombent sous le coup des nouvelles procédures plus sévères de ciblage qui sont décrites ci-dessous. Comme nous l'avions recommandé (Rapport annuel de 1986-1987, page 43), des critères détaillés qui nous satisfont ont été élaborés concernant l'ouverture de dossiers sur des particuliers et des groupes.

Deuxième suivi : le ciblage et les mandats judiciaires

Des mesures ont été prises à l'égard d'un certain nombre d'autres questions que nous avions soulevées l'an dernier dans le cadre de l'étude d'antisubversion. Le SCRS a établi un groupe de travail chargé d'examiner toutes les lignes de conduite et il refond actuellement son Manuel des opérations pour le faire concorder avec la *Loi sur le SCRS*.

En ce qui concerne les mandats judiciaires, le changement a été accéléré par la révélation en novembre dernier que le SCRS avait laissé des informations d'une source non digne de foi dans une demande qu'il avait présentée à la Cour fédérale, et que cette dernière avait agréée, en vue d'obtenir l'autorisation d'intercepter des communications téléphoniques pendant une enquête d'antiterrorisme. Le SCRS et l'inspecteur général ont entamé tous deux des examens approfondis des mandats judiciaires qui étaient alors en vigueur. En particulier, le Service a entrepris de vérifier et de justifier par écrit chaque allégation de fait figurant dans les demandes de mandats judiciaires. Nous avons l'intention de revoir cet exercice.

Ce qui est plus important pour l'avenir, un certain nombre de mesures ont été prises en vue d'améliorer les comptes rendus. Des coordonnateurs des mandats judiciaires s'assurent que toutes les lignes de conduite et procédures pertinentes sont respectées lorsqu'une demande est faite. Tous les faits qui sont exposés dans les affidavits sous-tendant les demandes reposent sur des preuves documentaires. Un nouveau certificat du contenu des affidavits attribue des responsabilités explicites à ses quatres signataires. Un analyste et chef de section certifient que la base de données du SCRS étaye les faits allégués. Un chef atteste la fiabilité des rapports dont les faits sont tirés et le besoin des pouvoirs demandés. Un directeur général atteste que l'information exigée par le paragraphe 21(2) de la *Loi* a été fournie.

Les demandes de mandats judiciaires doivent également donner de plus amples renseignements sur les pouvoirs qui seront exercés. Lorsqu'un renouvellement est demandé, l'analyste revoit les informations déjà obtenues au moyen des pouvoirs dont l'exercice a été

autorisé par le mandat judiciaire. Si aucun renseignement utile n'est survenu, il faut songer à utiliser des techniques d'enquête différentes.

La procédure de ciblage a également été améliorée. Comme pour les demandes de mandats judiciaires, des preuves documentaires doivent être présentées à l'appui des faits cités dans toute proposition en vue de cibler un particulier («Rapport d'évaluation d'un sujet» ou RES), et les opinions et recommandations doivent être distinguées des faits. Une «description complète et équilibrée» des activités de la cible proposée doit être fournie. Nous avons instamment recommandé (Rapport annuel de 1986-1987, page 42) que les RES soient «moins fondées sur des incidents isolés et donn[ent] davantage un exposé cohérent des raisons militant en faveur de la décision de ciblage recherchée de la part du CARC [Le Comité d'approbation et de réévaluation des cibles]».

Les conséquences pour la sécurité nationale si les pouvoirs demandés ne sont pas accordés—en d'autres termes, le besoin réel du mandat judiciaire—doivent aussi être prises en considération maintenant. Le Manuel des opérations révisé charge les enquêteurs de veiller à ce que l'on tienne compte des dommages aux droits et libertés constitutionnels qui pourraient résulter de l'utilisation de techniques comportant intrusion. Comme dans le cas des mandats judiciaires, lorsqu'une autorisation d'enquête accordée par le CARC expire, l'enquêteur demandant un renouvellement doit fournir un rapport d'évaluation indiquant s'il y a eu des changements dans les hypothèses initiales—si la cible est toujours capable d'atteindre ses objectifs, par exemple.

Le traitement des groupes a été modifié. Des enquêtes sont menées sur des personnes que nous avons appelées des «cibles de deuxième plan»—celles qui viennent à la connaissance du SCRS seulement parce qu'elles ont des contacts avec des cibles principales (Rapport annuel de 1986-1987, page 40)—dans le seul but d'identifier ces cibles. Des particuliers peuvent maintenant être ajoutés aux RES de groupe seulement avec l'approbation du CARC, plutôt que sur la demande d'un directeur général.

Le Comité d'examen des mandats judiciaires et le Comité d'approbation et de réévaluation des cibles (CARC) sont tous deux présidés personnellement par le directeur, et le Comité d'examen des mandats judiciaires comprend un avocat du ministère de la Justice qui se fait «l'avocat du diable», contestant le besoin de chaque mandat judiciaire demandé. Conformément à une recommandation que nous avons formulée dans notre rapport annuel de l'an dernier (page 42), un fichier centralisé de toutes les cibles est tenu.

Notre dernière réserve concerne le niveau auquel «l'avocat du diable» participe au processus d'examen des demandes de mandat judiciaire. Lorsque nous avons fait cette proposition (Rapport annuel de 1986-1987), nous avons suggéré que cet agent intervienne devant le solliciteur général ou la Cour fédérale elle-même. Dans la situation actuelle où l'avocat du diable n'est qu'un participant, dominé en nombre par les autres officiels du Comité d'examen de mandats judiciaires, nous pensons que la réforme n'est pas allée assez loin. Toutefois, nous sommes au courant que le rôle convenable de l'avocat du diable est en train d'être examiné avec une grande attention.

Il reste à voir jusqu'à quel point les nouvelles procédures sont respectées en pratique. Mais elles font certainement déjà beaucoup pour atténuer un grand nombre d'inquiétudes que nous avons déjà exprimées (Rapport annuel de 1986-1987, pages 40-42). Les premiers

signes sont encourageants. Nous avons examiné certaines demandes de mandats judiciaires qui ont été présentées après la réforme et, à première vue, nous sommes satisfaits des changements qui se sont produits. Comparativement à ce que nous voyions avant, ces demandes sont maintenant des modèles de précision, de clarté et de logique.

Un exemple typique

L'«Affaire Boivin» illustre certaines préoccupations que nous avons signalées par le passé—et une partie du travail que le SCRS avait déjà effectué, avant la récente avalanche de changements, pour faire concorder ses pratiques de ciblage avec la *Loi sur le SCRS*.

L'affaire a éclaté lorsque les médias ont rapporté que Marc-André Boivin, dirigeant syndical au sein de la Confédération des syndicats nationaux (CSN) qui était passible d'accusations liées à un attentat à la bombe devant les tribunaux du Québec, était une source du SCRS, peut-être un *agent provocateur*, et que ses activités illégales faisaient partie d'un complot du SCRS pour bouleverser et discréditer le mouvement ouvrier. Utilisant des renseignements recueillis par l'inspecteur général, nous avons examiné ces allégations et le solliciteur général a rendu notre rapport public le 29 mars 1988*.

Nous avons appris qu'en 1973 M. Boivin était devenu une source pour la GRC, qui lui avait donné instruction de surveiller les activités criminelles et «subversives» soupçonnées au sein du milieu ouvrier. À deux reprises, il avait eu maille à partir avec la justice relativement à son travail syndical—en 1973, pour avoir troublé la paix en piquetant et en 1978 pour avoir mis de la colle dans les serrures d'un immeuble public. Au moment de ce dernier épisode, la GRC a stipulé à M. Boivin qu'il ne se donne pas à des activités qui aillent à l'encontre des politiques de la gendarmerie, ou de la loi. En 1983, le module des affaires syndicales du Service de sécurité de la GRC n'enquêtait plus, il ne faisait que surveiller.

Lorsque le SCRS a pris la relève du Service de sécurité en 1984, M. Boivin n'avait plus comme cible le mouvement ouvrier. Il visait plutôt des communistes et des agents sous l'influence de pays étrangers qui essayaient d'infiltrer le mouvement ouvrier. Il est clair d'après les documents et les entrevues que le SCRS n'a pas ménagé ses efforts pour s'assurer que M. Boivin comprenait les limites de son affectation, à savoir qu'il n'était pas mandaté pour rapporter les activités des syndicats ou celles de leurs membres, sauf dans la mesure où elles étaient directement liées à l'influence communiste ou étrangère.

En fait, notre enquête a révélé que le SCRS n'avait chargé aucune source humaine de rapporter les affaires d'un syndicat ou les activités de syndiqués particuliers. Elle montrait également que les rapports de sources qui connaissaient le mouvement ouvrier ne portaient pas sur des questions comme les grèves, les organisations internationales, les syndiqués, les positions de négociation ou les objectifs généraux d'ordre politique, économique ou social.

Nous avons appris avec consternation que le SCRS avait attendu deux jours avant d'informer la *Sûreté du Québec* qu'il avait appris de M. Boivin qu'il y aurait des attentats à la bombe à Drummondville et à Montréal. Mais nous avons jugé que M. Boivin avait reçu

* *Rapport présenté, au terme de l'article 54, au solliciteur général du Canada sur l'usage par le SCRS de ses pouvoirs d'enquête en ce qui concerne le mouvement ouvrier.*

des directives appropriées du Service et que ce dernier n'avait pas essayé de le protéger à mauvais escient une fois que les accusations eurent été portées.

Nous avons aussi été perturbés de découvrir que le SCRS possède toujours des dossiers ouverts en 1970, avant la *Loi sur le SCRS*, époque où la GRC enquêtait toujours sur les syndicats. Le SCRS avait alimenté ces dossiers en conformité avec ses procédures normales. Même en l'absence d'une décision sur le ciblage, les recherchistes du SCRS versaient systématiquement au dossier pertinent, s'il y en avait un, tous les renseignements qu'ils trouvaient sur leur chemin. Nous avons aussi constaté que les enquêteurs du SCRS avaient pleinement accès à ces dossiers.

Le solliciteur général et le directeur ont pris des mesures que nous considérons appropriées. Les dossiers sur les syndicats ont été mis sous clé en vue d'être examinés et, s'ils ne respectent pas les dispositions de la *Loi*, ils seront détruits ou envoyés aux Archives nationales. Ordre a été donné de cesser la surveillance dans les cas où elle ne pouvait pas être justifiée en vertu de la *Loi*.

Sources ouvertes

L'utilisation, ou la sous-utilisation plutôt, des sources ouvertes par le SCRS constitue l'une de nos préoccupations continues. Par sources ouvertes, nous entendons des sources comme les médias et les journaux professionnels et techniques, au Canada comme à l'étranger, par opposition aux techniques comportant intrusion. Nous avons appris, par exemple, que l'ONA de l'Australie obtient de l'information des sources de renseignements et compte aussi fortement sur les médias comme les journaux et universités.

Le SCRS maintient et continue à ajouter un nombre de sources ouvertes dans son Centre d'information (antérieurement appelé le Centre de l'information de sources ouvertes), qui fournit des services de bibliothèque et de recherche dans les bases de données relatives aux enquêtes et analyses du SCRS. Mais la préférence pour les techniques d'enquête est endémiques au SCRS. Il semble avoir plus confiance dans les renseignements qu'il déniche pendant ses enquêtes que dans ceux qui sont à la portée de tout lecteur averti.

Le Groupe consultatif indépendant a réitéré nos préoccupations dans son rapport. En ce qui concerne l'une des rares recommandations que nous avions formulées dans notre dernier rapport annuel et sur lesquelles il n'était pas d'accord, le Groupe consultatif indépendant était d'avis que les recherchistes du SCRS ne devraient pas procéder à des recherches indépendantes ni préparer des résumés de l'information dans les dossiers. Mais il pensait généralement comme nous que le Centre d'information devait être mieux adapté aux activités des analystes des renseignements au SCRS. Il a noté que «le SCRS n'exploite pas à fond les sources ouvertes d'information» et affirmé que «des évaluations importantes de la menace, du moins au niveau stratégique ou environnemental, pourraient être faites principalement à l'aide de renseignements de sources ouvertes»*.

* Groupe consultatif indépendant sur le Service canadien du renseignement de sécurité, *Des ressources humaines et un processus en transition*, pages 20-21.

Il y a eu des changements appréciables depuis notre dernier rapport. Les documents en langue française constituent maintenant 28 pour cent de la collection du Centre—proportion qui, d'après les spécialistes en bibliothéconomie que nous avons consultés, est excellente pour une bibliothèque spécialisée de ce type. Cette augmentation était destinée non seulement à atteindre un certain quota linguistique, mais à garantir que tous les enquêteurs et analystes, non seulement ceux qui travaillent en français, auraient accès aux documents les plus utiles qui existent dans les deux langues officielles.

Il est difficile de faire des comparaisons d'année en année sur la manière de procéder des analystes pour avoir accès à l'utilisation des sources ouvertes par le Centre d'information puisque ce dernier a modifié sa façon de noter les documents qui sont consultés, mais il semble qu'une forte augmentation entre 1986 et 1987 ait résulté d'une demande accrue du Centre d'information de la part des sections administratives et techniques. Il semble y avoir eu une diminution à peu près correspondante dans la demande des analystes au sein des directions opérationnelles, même si les chiffres sont pondérés pour tenir compte du fait que des statistiques sur la Direction de l'antisubversion n'ont été recueillies que pendant une partie de l'année. Cependant, les statistiques ne tiennent pas compte de plusieurs documents de source ouverte que le Centre d'information distribue régulièrement aux divisions opérationnelles.

Les nouvelles des régions sont encourageantes. On forme des employés pour les centres de référence régionaux. Nous sommes aussi heureux de noter qu'il y a maintenant des centres de référence à Montréal, au sein du bureau régional d'Ottawa et à Toronto, lesquels sont tous dotés d'installations modernes pour extraire les données, et que des autres ouvriront bientôt à Vancouver et à Edmonton. Les enquêteurs dans les régions, pouvant obtenir plus facilement des informations de sources ouvertes, sont moins portés à exercer leurs pouvoirs comportant intrusion.

Statistiques sur les mandats judiciaires

Il y a eu une forte baisse dans le nombre de mandats judiciaires autorisés en 1987 (voir tableau 1). Cette diminution est dûe en partie à l'élimination de la majorité des mandats judiciaires d'antisubversion, ainsi qu'à l'introduction de nouvelles procédures d'autorisation de mandats judiciaires à la suite des difficultés avec le mandat judiciaire Atwal.

Tableau 1. Mandats judiciaires nouveaux et renouvelés au SCRS de 1985 à 1987

	1985	1986	1987
Nouveaux mandats judiciaires	82	94	71
Mandats judiciaires renouvelés	27	11	5
Total	109	105	76
Durée moyenne des mandats judiciaires (jours)	173.6	162.2	190.82

Source : SCRS

Les statistiques du tableau 1 suivent le modèle de tous nos rapports annuels précédents. Mais dans chacun de ces rapports nous avons dit que nous voulions trouver une manière de fournir des renseignements plus précis au sujet des mandats judiciaires sans porter atteinte à la sécurité nationale.

Nous avons essayé plusieurs moyens pour y arriver, mais chaque idée a avorté parce que le SCRS a maintenu sincèrement que si nous en révélions davantage cela donnerait une aide injustifiable à l'espionage ou au terrorisme.

Bien que nous ne soyons pas d'accord avec le SCRS, nous considérons son objection très sérieusement puisqu'il s'agit de la sécurité nationale. À la place, nous proposerons un format de statistiques qui, nous pensons, serait plus utile pour les Canadiens quand un Comité parlementaire commencera l'examen de cinq ans de la *Loi sur le SCRS*, qui est prévu pour l'an prochain. Le parlement lui-même décidera alors si la *Loi* aura besoin de publier des statistiques similaires à celles que nous proposerons ou si les préoccupations du SCRS concernant la sécurité nationale sont suffisament bien fondées pour rejeter notre proposition.

De toutes manières, nous tenons à assurer les Canadiens que nous continuerons à examiner tous les mandats judiciaires chaque année et que nous aviserons immédiatement le Solliciteur général et même s'il le faut le parlement, si selon nous, le SCRS abuse de ses pouvoirs.

Nous proposerons au Comité parlementaire que la *Loi sur le SCRS* exige des statistiques détaillant le nombre de citoyens canadiens ou de résidents permanents légaux qui ont été touchés—même marginalement, par les pouvoirs de surveillance accordés au SCRS en vertu d'un mandat judiciaire de la Cour Fédéral.

Étant donné que nous croyons que si on donnait le nombre exact de non-canadiens affectés par les mandats judiciaires cela pourrait peut-être porter atteinte à la sécurité nationale, nous ne proposons pas de rendre publique le nombre total de mandats judiciaires autorisés par la Cour fédéral entre ceux touchant les canadiens et ceux touchant les étrangers au Canada. Pour la même raison, nous ne proposons pas de rendre publique le nombre total de particuliers touchés par les mandats judiciaires.

Selon nous, la publication annuelle du nombre de canadiens et de résidents permanents légaux touchés par les mandats judiciaires de la Cour fédéral accordés au SCRS, fournirait au public des renseignements significatifs sur la manière avec laquelle le SCRS a exercé ses pouvoirs sans porter atteinte à la sécurité nationale. Nous pensons que de telles statistiques seraient beaucoup plus utiles, et probablement même moins susceptibles de porter atteinte à la sécurité nationale, que les chiffres que nous avons publiés cette année. Toutefois, nous attendons que le Parlement se prononce sur ce point avant de faire tout changement.

Filtrage de sécurité

Le délai dans le traitement des demandes d'habilitation de sécurité a continué à poser de sérieux problèmes en 1987-1988. Il faut toujours plus de sept mois pour effectuer les vérifications aux niveaux I (antérieurement appelé CONFIDENTIEL) et II (SECRET), et plus d'un an au niveau III (TRÈS SECRET). Le SCRS est le premier à reconnaître que ce délai est trop long; il convient que 30 jours serait raisonnable pour l'habilitation aux niveaux I et II, et le Comité croit qu'idéalement il en faudrait 90 pour le niveau III.

Pourquoi faut-il tant de temps? La réponse est simple : le SCRS est débordé. L'année dernière, il a traité environ 90 000 demandes de vérification touchant des immigrants éventuels, 90 000 demandes de vérification en matière de citoyenneté, 46 000 demandes en vertu de la Politique concernant la sécurité du gouvernement (PSG), 14 000 demandes visant des travailleurs d'aéroport et 7 000 demandes dans d'autres catégories.

Comme on l'avait prévu lorsque la PSG est entrée en vigueur en 1986, moins de demandes d'habilitation ont été présentées en vertu de cette politique. Les demandes ont diminué de plus du tiers par rapport au niveau de 1986-1987. Il y a aussi eu une baisse sensible dans le nombre de longues enquêtes sur le terrain qui étaient requises.

Mais, si le SCRS espérait que cela réduirait sa charge de travail, le ministère des Transports a anéanti ses espoirs en exigeant des cotes de sécurité pour tous les travailleurs d'aéroport ayant accès aux zones limitées, comme mesure d'antiterrorisme. On a reconnu dès le début que l'attribution de ces cotes devrait s'étaler sur plusieurs années, à compter de 1987-1988. L'objectif de la première année était de 10 000 cotes. Pour la première année on s'attend qu'il soit de 24,000 à 28,000 demandes. Déjà sur les dents, le SCRS a dû faire face à une demande de 240 pour cent du niveau attendu.

Le nombre d'événements internationaux majeurs qui ont eu lieu au Canada est venu compliquer temporairement les choses. Près de 600 cotes du niveau II étaient requises pour la réunion des chefs d'État du Commonwealth qui s'est déroulée à Vancouver des 13 au 17 octobre et environ 500 pour le Sommet économique qui devait avoir lieu à Toronto à la mi-juin de 1988.

La Direction du filtrage de sécurité est également victime des installations physiques insuffisantes fournies au SCRS. Les analystes ne sont pas logés dans les mêmes locaux que les dossiers qu'ils doivent consulter. Pendant que des terminaux d'ordinateur restent dans leurs emballages parce que tout le monde est trop occupé pour veiller à leur installation, les employés de la Direction font la queue pour se servir des terminaux qui sont branchés. Bien des postes dans la Direction sont vacants.

Il n'est pas surprenant que, malgré la prestation de ressources additionnelles, l'arriéré de travail reste énorme—43 000 vérifications en matière de citoyenneté, 33 000 vérifications en matière d'immigration et 15 000 cotes de sécurité en vertu de la PSG. Reconnaissant qu'il était dépassé par les événements, le SCRS a fait appel à un expert du Conseil du Trésor, qui a examiné comment le système pouvait être simplifié, déterminé les ressources supplémentaires qui s'imposaient. Les recommandations contenues dans le rapport de l'expert sont en vigueur. Le SCRS a montré sa créativité et sa flexibilité, et il a même trouvé d'autres améliorations à celles du rapport.

Un changement important en matière de filtrage de citoyenneté est que les responsabilités du SCRS diminuent, ce qui permettra à la Direction du filtrage de sécurité d'utiliser mieux ses ressources puisque les demandes de vérification de citoyenneté représentaient un tiers de toutes les demandes de vérifications.

Le SCRS prévoit que d'ici la mi-juillet 1988, tout l'arrérage des demandes, y compris toutes celles de filtrage, ne sera que de 35,000 à 40,000, au total, ce qui représente moins de la moitié du nombre d'il y a six mois.

4. Le SCRS lui-même

Notre dernier rapport annuel et notre rapport spécial sur les langues officielles et les relations de travail au SCRS, *Pour corriger une situation*, de même que le rapport subséquent du Groupe consultatif indépendant du solliciteur général, ont tous eu une incidence de taille l'an dernier sur la façon dont le SCRS mène ses affaires internes. L'année n'a pas été facile pour le Service, mais nous avons remarqué des améliorations considérables qui faciliteront les choses à l'avenir. Le présent chapitre en expose les points saillants.

L'Académie, hier et aujourd'hui

Nous avons été heureux d'apprendre que le SCRS avait décidé de rouvrir l'académie Sir William Stephenson en avril 1988. L'Académie est l'école où le SCRS forme ses nouveaux agents de renseignements (AR); c'est la porte par laquelle une nouvelle génération pénètre dans le domaine du renseignement de sécurité.

Nous avions été profondément déçus d'apprendre au printemps de 1987 que l'Académie fermerait ses portes pour un an. Après avoir embauché un grand nombre d'agents de renseignements au niveau AR-3 à l'automne de 1986, le SCRS a affirmé qu'il n'avait plus d'argent pour former une classe de AR-1 à l'Académie pendant l'année financière 1987-1988. Ce que nous n'avons pas aimé c'est que presque tous les agents embauchés à l'automne de 1986 étaient d'anciens policiers. Entrant à un niveau plus élevé que les recrues civiles qui étaient formés à l'Académie, ils avaient de meilleures chances d'avancement. Il nous semblait que le SCRS ratait l'occasion de diversifier les antécédents et l'expérience de son personnel.

Mais, en 1987-1988, le SCRS a cessé d'embaucher ses AR de cette façon, comme il l'avait promis. Les seuls nouveaux employés qui ne sont pas passés par l'Académie étaient des gestionnaires intermédiaires ou supérieurs ayant des compétences spécifiques dont le Service avait besoin. En même temps, on dressait des plans en vue de permettre aux agents comptant de nombreuses années de service de prendre une retraite anticipée et de faire ainsi de la place pour du sang nouveau.

Quant au programme de l'Académie, nous avons toujours été enthousiastes. Même si une grande partie de la période de transition, pendant laquelle le SCRS a pris la relève du Service de sécurité de la GRC, a été marquée par les bouleversements et les retards, nous avons dit dans notre Rapport annuel pour 1985-1986 qu'«il est particulièrement impressionnant de constater avec quelle rapidité le Service a réussi à créer à partir de rien un programme de formation qui a reçu une très bonne évaluation de la part de sa première promotion de recrues». Le SCRS va chercher les conférenciers de l'Académie non seulement dans le secteur de la sécurité et du renseignement mais aussi dans les universités et au sein de l'Association canadienne des libertés civiles. À la fin de l'année, un de nos collègues, Jean Jacques Blais, devait expliquer le rôle de notre comité à la classe d'avril 1988.

Représentation et bilinguisme

À la fin de l'année, la classe d'avril 1988 avait eté constituée. Ne comptant que 12 recrues, elle est très petite—en fait, c'est la plus petite classe que l'Académie ait jamais eue. Mais il s'agit néanmoins d'un pas en avant. Rendre le Service plus représentatif de la société

qu'il sert constitue un objectif de recrutement important. Nous trouvons la composition de cette classe rassurante (tableau 2).

Tableau 2. Composition des classes à l'académie Sir William Stephenson

	Sexe		Première langue officielle		Source	
	M	F	A	F	Extérieur	Conversion
janv. 1986	25	8	32	1	33	0
févr. 1986	9	5	8	6	0	14
juin 1986	16	4	18	2	20	0
sept. 1987	5	2	3	4	0	7
févr. 1987	18	2	14	6	20	0
avr. 1988	4	8	6	6	9	3

Source : SCRS

En ce qui concerne sa répartition linguistique et par sexe, la classe n'est pas aussi disproportionnée qu'elle peut le paraître à première vue. C'est ce dont le SCRS a besoin s'il doit devenir plus représentatif de la population canadienne. Comme l'une de nos collègues, Paule Gauthier, l'a fait remarquer dans une allocution qu'elle a prononcée devant l'Association des femmes juristes du gouvernement fédéral le 13 janvier 1988 : «Le monde de la sécurité nationale n'est pas un monde où les femmes sont bien représentées. Certes, il y a eu, dans l'histoire, des femmes qui ont joué des rôles d'espionne de façon magistrale mais le nombre de femmes actives à divers échelons de la direction du Service de sécurité est très minime, pour ne pas dire quasi inexistant».

Pour ce qui est de la première langue officielle, le SCRS a encore du travail à faire avant de pouvoir fonctionner efficacement aussi bien en français qu'en anglais et être représentatif de la population canadienne. Nous somme heureux d'affirmer que toute la classe est bilingue.

Quant à la catégorie «source» au tableau 2, les neuf recrues provenant de l'extérieur du Service viennent de terminer leurs études universitaires. Les trois autres sont des agents de surveillance du SCRS «convertis» au groupe AR. Nous avons déjà longuement commenté (*Pour corriger une situation*, chapitre 15, Rapport annuel de 1986-1987, pages 52-53) les problèmes de moral que pouvaient avoir les agents de surveillance—les gens qui filent les cibles du SCRS—parce que leur travail ne mène pas normalement à des promotions. Nous croyons qu'il est juste que le SCRS fournisse aux surveillants ayant les compétences voulues des chances raisonnables d'accès à la catégorie des AR, où il y a plus d'avancement.

Il faudra encore veiller à la représentation des minorités ethniques et visibles et des peuples autochtones. Nous croyons qu'il est essentiel que ces groupes soient bien représentés.

Il est important qu'ils considèrent le SCRS comme un environnement dans lequel leur peuples et leurs valeurs seront respectés. D'ailleurs le SCRS a besoin des aperçus qu'ils peuvent lui apporter concernant la réalité de la société multiculturelle et multiraciale qui existe aujourd'hui au Canada. Il est toujours difficile de trouver des renseignements statistiques fiables sur l'ethnicité. Mais on se rend compte immédiatement que les minorités ethniques et raciales et les peuples autochtones ne sont pas bien représentés au SCRS. Il est évident qu'on doit s'efforcer de réaliser une représentation plus juste.

Nous constatons que la GRC a créé une équipe de recrutement national qui, pour reprendre les paroles prononcées par le solliciteur général le 28 mars 1988, «apporte le message aux minorités et aux peuples autochtones que la GRC s'intéresse à eux pour qu'ils fassent une carrière comme représentant de la loi». La GRC avait déjà lancé une campagne s'adressant aux femmes et aux francophones. Les circonstances de la GRC et du SCRS sont très différentes, évidemment; nous l'avons souvent fait remarquer nous-mêmes. Mais nous notons avec intérêt que la GRC a décidé d'aller au-devant des gens qu'elle veut plutôt que d'attendre qu'ils viennent à elle. Nous remarquons aussi avec intérêt que la GRC vise à recruter 5 pour cent de son effectif parmi les minorités visibles.

L'utilisation du polygraphe : De mal en quoi?

Les nouvelles au sujet d'un autre thème sur lequel nous revenons souvent nous préoccupent quelque peu. Nous nous sommes opposés à maintes reprises à l'utilisation du polygraphe au sein du SCRS (Rapport annuel de 1986-1987, page 53; Rapport annuel de 1985-1986, page 19). Nous ne reprendrons pas notre argument en détail ici. Qu'il suffise de dire que même les partisans du polygraphe avouent un taux d'erreur d'au moins 10 pour cent. Le polygraphe enregistre les manifestations physiques de tout genre d'émotion; il enregistre la crainte ou la contrariété de la même façon qu'il enregistre la culpabilité. Le «résultat» du test est une interprétation par un opérateur de ce que dit la machine. Dans le meilleur des cas, l'opérateur porte un jugement professionnel; dans le pire, il ne fait que deviner.

Nous ne croyons pas nécessairement que la marge d'erreur ne soit que de 10 pour cent. Mais, même en admettant que cela soit vrai à des fins de discussion, il faut reconnaître qu'un résultat erroné sur 10 serait considéré comme un taux d'erreur très élevé dans la plupart des domaines. Ce taux est, en réalité, trop élevé pour justifier le vernis scientifique dont le polygraphe peut enduire des décisions arbitraires et préjudiciables au sujet des carrières de Canadiens loyaux.

L'an dernier, nous avons été heureux de rapporter que le SCRS n'administre plus systématiquement des tests du polygraphe aux personnes qui font déjà partie de son effectif. Mais la situation s'est encore améliorée depuis lors. Les recrues éventuelles doivent maintenant subir le test du polygraphe seulement pour la loyauté et plus sur leur style de vie.

Les défenseurs de ces tests aiment à répéter que les tests du polygraphe ne sont qu'une parmi de nombreuses procédures de filtrage auxquelles les recrues éventuelles doivent faire face. Cela est vrai. Mais nous ne pouvons croire qu'une lecture défavorable du polygraphe est ignorée lorsqu'elle est contredite par des preuves d'autres sources. Cela ne cadre pas avec notre façon de voir la nature humaine au XX^{e} siècle, nourrie dans la conviction que «la science a réponse à tout». Il serait difficile, voire impossible, pour les responsables du

recrutement, même avec la meilleure volonté du monde, de conclure à la fidélité au Canada d'une recrue en face d'une machine apparamment scientifique qui dit le contraire.

Au delà du dommage causé à des carrières en herbe dans le secteur du renseignement de sécurité et de la tache qui demeure sur le dossier de ceux qui «ratent» le test, une question plus vaste se pose. Si le SCRS et ses maîtres au gouvernement considèrent le polygraphe comme suffisamment fiable pour être utilisé pendant le processus de recrutement, dans combien de temps commenceront-ils à en étendre l'application? Son utilisation pour les enquêtes sur la sécurité peut-elle être bien loin? Quand le secteur privé emboîtera-t-il le pas au gouvernement? Dans combien de temps le test du polygraphe deviendra-t-il obligatoire pour des millions de Canadiens? Ce n'est pas là le genre de société que le SCRS a été chargé de protéger.

Nous avons vivement recommandé «la réalisation d'une étude approfondie et objective qui permettrait au solliciteur général et au gouvernement de décider pour eux-mêmes si l'utilisation de pareilles méthodes est compatible avec les valeurs d'une société libre et démocratique» (Rapport annuel de 1986-1987, page 55).

Un comité interministériel s'est penché sur cette question en 1987-1988. Il a demandé à un consultant indépendant d'examiner la recherche qui avait été effectuée pour lors à cet égard. Fort bien. Malheureusement, la hâte avec laquelle nous avons appris que le travail avait été fait est évidente. Le consultant ne traite pas du tout les conclusions d'une importante commission royale en Ontario* qui a spécifiquement étudié la question des tests du polygraphe sur les lieux de travail, et il ne fait que mentionner en passant les témoignages concernant une loi ontarienne de 1983 qui interdit les tests du polygraphe pour le filtrage du personnel**.

Même si le consultant examine tant les avantages que les inconvénients du polygraphe sans arriver explicitement à aucune conclusion ferme, nous mettons en question l'objectivité d'un rapport qui décrit les tests du polygraphe comme «une forme de test psychologique». Pour ce qui est de la fiabilité scientifique du polygraphe, cette description ne tient pas debout si l'on considère que les personnes qui administrent les tests du polygraphe ne sont pas tenues d'avoir reçu une formation de psychologue. En fait, le SCRS se sert de psychologues pour administrer ses tests du polygraphe. Cela vaut mieux que rien. Mais le recours à des psychologues n'est pas une norme universelle à laquelle on doit s'attendre que les autres utilisateurs du polygraphe, à l'intérieur ou à l'extérieur du gouvernement, se conforment automatiquement.

À la lumière de l'expertise à notre disposition, nous nous opposons à ce que les tests du polygraphe soient décrits comme «une forme de test psychologique» lorsqu'ils manquent de valeur, de fiabilité et de comparabilité et lorsque les réactions des particuliers sont interprétées d'après une procédure qui ne dure normalement qu'environ deux heures.

---

* Le juge Donald Morand, *Report of the Royal Commission into Metropolitan Toronto Police Practice*, Toronto 1976

** *Loi modifiant la Loi sur les normes d'emploi*, troisième session, 32e législature, Ontario

À la fin de 1987-1988, les événements semblaient sur le point d'aboutir. Le comité interministériel avait reçu un rapport d'un groupe de travail et exposait les options dans un document destiné au Comité interministériel de la sécurité et des renseignements (CISR), constitué à l'échelon des sous-ministres. Nous n'avons vu ni l'un ni l'autre de ces documents (ils débordent le cadre de notre mandat de surveillance). Mais nous espérons que le CISR ne prendra aucune décision fondée uniquement sur le rapport du consultant que nous avons vu et que nous considérons inadéquat. Nous espérons qu'il procédera plutôt à d'autres enquêtes—et consultera en particulier des experts en matière d'épidémiologie statistique.

Gestion

Un certain nombre de changements ont été apportés à la gestion du SCRS. Le cabinet du directeur comprend maintenant un secrétariat responsable de la planification et de la coordination et des liaisons avec le Comité de surveillance des activités de renseignement de sécurité, l'Inspecteur général, les ministres et la Chambre. Le secrétariat est aussi chargé de l'organisation et du soutien des comités, et du CARC. Le directeur préside personnellement tous les principaux comités de gestion interne.

Ces comités comprennent le Comité de gestion des ressources humaines. La fonction «personnel», qui comprend les questions liées aux langues officielles, est maintenant coiffée par un sous-directeur plutôt que par un directeur général, et on nous assure qu'un plan exhaustif des ressources humaines, portant sur la formation et le perfectionnement, les langues officielles et les objectifs de recrutement, est en voie d'élaboration.

Dans *Pour corriger une situation*, nous avons instamment recommandé la création temporaire d'un poste au niveau de sous-directeur dont le titulaire serait chargé de mettre en oeuvre un plan spécial visant les langues officielles. Étant donné les événements qui sont survenus depuis lors, notamment la nomination d'un nouveau sous-directeur du personnel et des langues officielles, nous sommes d'avis que cette mesure n'est plus nécessaire.

Nous avons déjà attiré l'attention du gouvernement sur une question clé dans le domaine du personnel, à savoir les possibilités d'échanges entre le Service et la Fonction publique du Canada. Parce que cette mesure exigerait des modifications statutaires, elle dépasse les pouvoirs du SCRS, et nous y revenons au chapitre 10.

Quant aux questions sans le contrôle du SCRS, il nous semble que le Service resserre son système de gestion d'une façon qui pourrait lui éviter certains problèmes qui se sont posés par le passé.

5. Opérations d'antiterrorisme

L'Antiterrorisme (AT) constitue l'une des deux directions opérationnelles du SCRS,* et nous en avons fait une étude approfondie en 1987-1988. Un rapport circonstancié sera remis au Solliciteur général et au directeur du SCRS. Il s'agit d'un long document dont les recommandations sont cotées. Le présent chapitre en donne, dans la mesure du possible, les grandes constatations et conclusions.

Mandat du SCRS

La principale question à trancher pour d'autres enquêtes dans ce domaine consiste à décider ce que veut dire le mot «terrorisme». Dans une étude savante, on trouve plus de 100 définitions. Pour le SCRS, cependant, la difficulté est simplifiée, son mandat à cet égard est énoncé clairement au paragraphe 2c) de la *Loi sur le SCRS* : «les activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage de la violence grave ou de menace de violence contre des personnes ou des biens dans le but d'atteindre un objectif politique au Canada ou dans un État étranger.»

Pour lutter contre le terrorisme, comme contre toute autre menace envers la sécurité du Canada énumérée à l'article 2, le SCRS a pour mandat, en vertu de l'article 12 de la *Loi*, de «recueillir, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et d'analyser et de conserver les informations et renseignements», de «faire rapport au gouvernement du Canada et de le conseiller à cet égard.»

Il importe de signaler que le SCRS *ne* détient *pas* de mandat pour faire respecter le droit criminel ou réunir des preuves en vue de poursuites criminelles. Cette notion ne semble pas être très claire dans l'esprit de certains critiques du Service. Le SCRS cherche à découvrir les sources et les cibles du terrorisme et les autres menaces envers la sécurité du Canada. Mais la protection des cibles et l'arrestation des criminels relèvent, de toute évidence, des corps policiers, notamment de la GRC en vertu de la partie IV de la *Loi sur le SCRS* (appelée *Loi sur les infractions en matière de sécurité*).

Points et méthodes étudiés

Nous avons entamé notre étude en ayant en tête quatre questions. Premièrement, le SCRS joue-t-il son rôle dans la protection des Canadiens contre le terrorisme? Pour répondre à cette question, nous nous sommes penchés sur la capacité de la Direction de l'AT à déceler les causes apparentes de l'activité terroriste, à analyser leur importance, à réunir les renseignements pertinents et à transmettre ces renseignements à ceux qui sont chargés de faire échec aux menaces terroristes à temps.

La deuxième question portait sur l'activité du SCRS dans le respect de la loi, à savoir non seulement la Loi elle-même, mais également les mandats et les directives ministérielles. Il s'agissait de comparer les politiques et les méthodes du Service avec ces mécanismes de contrôle et de comparer les pratiques régionales aux politiques et aux méthodes. Il y a également des questions de responsabilité : à savoir si chaque intervenant, de l'enquêteur

* L'autre est le Contre-espionnage (CE). Nous l'étudierons l'an prochain et publierons nos conclusions et constatations dans notre prochain rapport annuel.

régional au directeur, détient les attributions qui conviennent à son rang dans la hiérarchie.

Troisièmement, nous nous sommes demandés si le Service se servait de ses pouvoirs de façon abusive ou inutile dans le cadre du programme d'AT. Nous nous sommes préoccupés tout particulièrement des interventions du Service qui pourraient nuire aux activités politiques, culturelles ou sociales des groupes ethniques.

Enfin, nous nous sommes demandés si la *Loi* offrait un cadre législatif adapté aux activités du SCRS dans ce domaine. Ce point est d'actualité. Toute imperfection du mandat du SCRS peut être rectifiée l'an prochain quand le Parlement canadien fera l'examen de la *Loi sur le SCRS* (L'examen quinquennal est traité au chapitre 10 du présent rapport).

L'étude exécutée par le CSARS a compris : l'examen de l'infrastructure de la Direction de l'AT, et des ressources financières et humaines dont elle dispose, l'interrogation des officiers du SCRS qui exécutent le programme d'AT à la grandeur du pays et l'examen des nombreuses sources de renseignements qu'utilise le Service, la consultation des dossiers opérationnels, et la lecture de documents dont le sujet varie du décèlement de menaces latentes jusqu'à l'analyse d'activités passées.

Notre étude a porté sur le recours aux ressources et aux pouvoirs d'intrusion selon la cible et la région. Nous avons établi des comparaisons d'une année par rapport à l'autre. Nous avons examiné des indices de l'emploi de moyens clandestins pour recueillir des renseignements et nous avons posé des questions à propos de l'acceptabilité de ses moyens vis-à-vis les différentes cibles d'enquête.

Le défi

Le premier défi que doit relever toute enquête d'antiterrorisme se situe dans la difficulté de réunir de l'information. Souvent, les groupes terroristes se divisent en cellules, groupements fermés et cohérents difficiles à infiltrer. Il est dangereux de trop se rapprocher des gens qui ont recours à la violence pour atteindre leurs objectifs. Cette proximité, excessive sur le plan de la sécurité, est à peine suffisante quand il s'agit de réunir de l'information. On raconte que certaines organisations terroristes n'accepteront de nouveaux membres dans leur cellule seulement après qu'ils aient commis des actions de violence criminelle. L'origine de l'information utile aux opérations d'AT est, forcément, un secret étroitement surveillé.

Le changement est un autre défi que doit relever l'AT. Le personnel affecté au terrorisme, les méthodes et les objectifs dans ce secteur se sont transformés avec le temps. Les menaces terroristes qui font l'objet d'enquêtes aujourd'hui étaient en majeure partie insoupçonnées au Canada il y a 10 ans. Dans 10 ans, seront-elles celles d'aujourd'hui? La Direction de l'antiterrorisme ne peut prétendre en toute sécurité que ce sera le cas. En plus de faire enquête sur les terroristes d'aujourd'hui, un service de renseignement doit toujours se tenir aux aguets des dangers latents.

Les événements qui peuvent engendrer des menaces terroristes à venir peuvent survenir à l'extérieur du Canada. La plupart, mais non pas la totalité, des menaces terroristes envers la sécurité du Canada sont associées à des conflits qui font rage dans d'autres pays. Et

c'est là le troisième défi du SCRS : se tenir au courant d'événements qui surviennent dans des pays lointains, des événements qui peuvent être l'expression de siècles de conflits humains.

Le caractère international du terrorisme soulève des défis additionnels de part sa nature même. Dans la mesure où l'activité terroriste au Canada vise des cibles qui représentent, de façon réelle ou symbolique, des intérêts de nations étrangères, ces nations portent un certain intérêt à l'activité terroriste possible au Canada. Le SCRS peut profiter des échanges de renseignements avec ces pays, mais il doit éviter de tomber dans deux pièges. Le premier est de leur fournir des renseignements qui serviront à des fins répréhensibles. L'autre est d'accepter à première vue des renseignements faux, «de la désinformation», que ces pays peuvent offrir dans l'espoir d'utiliser le Canada à leurs propres fins.

Priorité accrue

Depuis sa création en 1984, le SCRS a mis sur l'AT un accent dont la croissance est phénoménale. La tragédie aérienne d'Air India a changé radicalement la façon de penser des Canadiens au sujet du terrorisme international, ainsi que le programme d'AT du SCRS. Le 23 juin 1985, un avion gros porteur d'Air India, parti de Toronto et de Montréal à destination de Bombay, s'est abîmé au large des côtes de l'Irlande, entraînant dans la mort les 329 personnes à son bord. La plupart des victimes étaient des Canadiens. Le gouvernement canadien n'a pas établi officiellement encore la cause, mais dans le public, la violence terroriste est au coeur des conjectures.

Pendant cette même période où les ressources étaient comprimées à l'échelle du gouvernement, l'administration du SCRS a d'abord tenté de faire face à un accroissement de la demande en matière de renseignements sur le terrorisme avec le programme d'AT dans sa forme initiale. Dans certains bureaux, les heures supplémentaires ont atteint des chiffres incompatibles avec une saine gestion du personnel et une utilisation efficace des ressources publiques. Il a fallu reporter de nouveaux programmes qui visaient à traiter plus efficacement l'information brute et à améliorer la sensibilisation du personnel régional à l'aspect culturel.

Mais on ne pouvait pas étirer indéfiniment les ressources en place et on a dû éventuellement passer à un nouveau plan d'attaque. Le SCRS a remanié ses ressources, déplaçant gens et biens pour exécuter les travaux prioritaires d'AT. On insista davantage sur la familiarisation des agents de renseignement avec les racines du terrorisme ethnique. Les méthodes furent améliorées afin de déceler les menaces latentes et de gérer celles à long terme. Des mécanismes furent perfectionnés afin de coordonner les événements spéciaux et on améliora les communications avec les autres services du gouvernement.

Voilà toute une batterie d'améliorations. Lorsque des innocents sont victimes d'attaques terroristes, le public a le droit d'exiger la meilleure protection possible. De bons renseignements sont les premiers éléments essentiels pour faire échec au terrorisme. Par conséquent, nous favorisons un programme d'AT solide.

Ciblage et enquêtes

Pour notre étude, nous avons examiné la politique et les méthodes de ciblage figurant dans le Manuel des opérations du SCRS, ainsi que dans tous les documents utilisés pour choisir une cible; et nous avons procédé à une vérification de sept décisions précises en matière de ciblage. Notre choix des sujets s'est fait en majeure partie au hasard. Quant aux mandats autorisant des techniques d'intrusion telles que l'écoute téléphonique pour faire enquête, nous avons vérifié tous les mandats que l'AT avait en main, procédé à des examens fouillés de certains, et consulté la politique et les méthodes énoncées dans le Manuel des opérations au sujet de demandes adressées à la Cour fédérale.

De plus, nous avons procédé à un examen exhaustif de six enquêtes menés par le SRCS, y compris et la surveillance à long terme de groupes ou de personnes soupçonnés de se préparer à de la violence à des fins politiques et des examens succincts au sujet d'incidents ou d'événements ayant des répercussions sur la sécurité nationale.

Les demandes en matière de mandat et de ciblage constituent des domaines où des transformations phénoménales sont survenues en 1987-1988, en raison de «l'affaire du mandat Atwal» (voir la page 17 du présent rapport annuel). Des révisions apportées au Manuel des opérations ont désormais apaisé les grandes préoccupations que nous formulions au sujet du ciblage dans notre étude du programme d'antisubversion (rapport annuel 1986-1987, pages 40-43).

Aujourd'hui, l'appartenance à un groupe soupçonné de violence à des fins politiques n'est pas un motif suffisant en soi pour cibler une personne à prime abord. Elle peut, bien sûr, attirer l'attention du SCRS sur cette personne. Mais les décisions en matière de ciblage sont prises en fonction du comportement individuel, non de l'affiliation à un groupe. Nous estimons que c'est là la façon qui convient d'aborder cette question. Comme nous l'avons indiqué clairement dans le rapport annuel de l'an passé, nous ne pensons pas que les gens devraient être ciblés uniquement parce qu'ils sont membres de groupes; le ciblage ne doit pas ignorer la nature ou l'importance de la participation personnelle.

Même si les nouvelles politiques en matière de ciblage et d'enquête assurent toutes les protections réclamées par nous dans le passé, elles suscitent des inquiétudes contraires chez les enquêteurs régionaux. Ils craignent que si toutes leurs activités doivent porter sur des menaces reconnues envers la sécurité du Canada, les menaces latentes leur échappent. Ils devraient pouvoir obtenir des renseignements, sans recourir à des techniques d'intrusion, qui permettront au Service d'établir ses priorités à venir en matière d'enquêtes. Au moment de la rédaction du présent rapport, le Service s'affairait à parachever les derniers détails de mise en oeuvre des politiques. Nous prônons l'adoption d'une interprétation sensée afin que les enquêteurs régionaux puissent poursuivre dans la voie menant vers une prévision de plus grande portée des menaces terroristes.

Nous souscrivons en général à la façon dont la Direction de l'AT utilise ses ressources. À part l'exception traitée plus loin dans ce chapitre, les priorités accordées aux diverses menaces terroristes semblent correspondre aux dangers qu'elles présentent. Fait également important, les priorités arrêtées par la Direction tiennent compte des menaces à long terme aussi bien qu'immédiates. Ainsi, pendant que se déroulait notre étude, la Direction, en

réaction à des événements nouveaux survenus à l'étranger, a augmenté la priorité accordée à une forme de terrorisme qui n'a jamais produit d'actes de violence au Canada.

L'étude a porté sur l'utilisation de sources humaines dans le domaine de l'AT. Le recrutement et le traitement de ces personnes constituent une tâche fort délicate. En plus des faiblesses connues de la nature humaine, les enquêteurs du SCRS doivent compter parmi leurs préoccupations la motivation et la fiabilité.

Nous avons constaté que l'AT prend grand soin, tant dans sa politique que dans la pratique, d'affecter ses sources uniquement à des cibles dûment désignées et à ne réunir que le genre de renseignements qui correspondent exactement à ce dont le SCRS a besoin en vertu de la *Loi*. Nous avons jugé satisfaisante la politique du SCRS en matière de recrutement des sources humaines, d'élaboration des sources et de vérification des dépenses, et nous n'avons relevé aucun manquement à cet égard.

Notre examen de la surveillance physique a compris des entretiens avec des agents chargés de ce travail, une revue du Manuel des opérations, un examen des vérifications internes du programme et une consultation de tous les rapports de surveillance établis dans deux régions au cours d'une période d'un mois en regard des cibles d'AT. Nous avons été fort impressionnés par la compétence et l'originalité avec lesquelles l'activité de surveillance a été exécutée.

L'étude s'est penchée sur l'emploi de moyens techniques d'interception, dont le traitement de renseignements obtenus de sources techniques. En décembre dernier, au cours de l'enquête sur la tragédie d'Air India, il a été dévoilé que le SCRS avait effacé des bandes magnétiques. Une politique qui régit le fonctionnement du SCRS prévoit la conservation d'éléments de preuve d'un crime. Elle prévoit également le signalement à la police de la découverte de toute situation périlleuse. En général, cependant, la politique exige qu'on transcrive l'information pertinente interceptée puis qu'on efface les rubans. Ainsi l'information sur des conversations privées, qui n'ont rien à voir avec la sécurité du Canada, n'est pas conservée. Au moment où nous écrivons nous n'avons pas encore pris de décisions finales concernant l'effacement des bandes magnétiques dans la tragédie d'Air India.

Politiques et pratiques

La collecte de renseignements est ce que le SCRS accomplit de mieux. Notre recherche nous a convaincus que la qualité générale des renseignements réunis par la Direction de l'AT est très bonne. La Direction présente une fiche louable dans la surveillance des déplacements et des activités de ses cibles.

Elle affiche également un scepticisme salutaire à l'égard des renseignements qu'elle obtient des organismes étrangers de renseignement. Il se produit inévitablement des chasses aux chimères en raison de renseignements inexacts ou trompeurs fournis par d'autres organismes; l'AT est un secteur où des erreurs peuvent coûter des vies, on ne peut donc négliger aucun renseignement. Cependant, la Direction tient compte des politiques étrangères des pays qui lui fournissent des renseignements et qui peuvent tenter de tourner les activités canadiennes d'AT à leur avantage. Elle tient également compte du dossier de référence des organismes étrangers qui, dans le passé, lui ont fourni des renseignements qui se sont révélés valables ou non.

Dans le cadre de ses enquêtes permanentes, la Direction de l'AT ne s'immisce pas indûment dans les affaires des collectivités ethniques. Elle concentre son attention sur les menaces bien arrêtées envers la sécurité nationale, non pas sur des groupes ethniques complets. Nous avons pris connaissance d'un cas où le SCRS a reçu à maintes reprises des demandes de conseils formulées par des membres d'un groupe ethnique sur les ripostes que la majorité modérée pourrait utiliser pour empêcher qu'une minorité manipule, à des fins politiques, des activités collectives. Le SCRS a répondu de façon retenue et convenable.

Les factions canadiennes de groupes étrangers, qui commettent des actes terroristes afin de renverser le gouvernement de leurs pays présentent un problème. En vertu de la *Loi sur le SCRS*, le Service doit réunir de l'information «dans la mesure strictement nécessaire». Quoique les sympathisants canadiens appuient l'objectif des terroristes étrangers, leurs activités ici se limitent surtout, dans bien des cas, à des manifestations et à des protestations politiques. Tous les conflits à l'étranger n'aboutissent pas à des attaques terroristes à l'échelle internationale.

Là où il n'y a pas danger apparent de violence au Canada, le Service doit veiller spécialement à ne pas faire enquête sur «les causes légitimes défendues ou les désaccords légitimes manifestés», sauf s'il s'agit de menaces terroristes. Il doit également se tenir au courant des menaces qui s'atténuent : à savoir, au fur et à mesure que le conflit violent à l'étranger s'apaise, il doit diminuer ses enquêtes sur les groupes de sympathisants canadiens, ou les réduire proportionnellement. C'est surtout indispensable dans des endroits comme les pays d'Amérique latine en conflit où les idéologies politiques oscillent constamment. Notre étude a relevé un cas où nous avons conclu que le Service avait mis trop de temps à se désintéresser d'un groupe de ce genre quand la contribution de celui-ci au conflit à l'étranger s'était amenuisée. Même si la *Loi* autorisait le ciblage de membres de ce groupe, nous sommes d'avis que la portée de l'enquête était exagérée.

Nous entretenons également certaines inquiétudes au sujet d'activités liées à des manifestations spéciales comme la réunion des chefs d'État du Commonwealth. Avant la tenue de telles rencontres, la Direction de l'AT interroge les membres les plus en vue des groupes ethniques où l'on retrouve des éléments minoritaires terroristes. Ces entrevues visent à réunir des renseignements sur des menaces possibles.

Mais elles ont un effet secondaire : elles rappellent à tous ceux qui font partie du groupe que le SCRS les surveillent et elles visent, par conséquent, à décourager les extrémistes. Tant mieux si elles y réussissent. Nous craignons toutefois que cet effet restrictif ne s'étende à tout le groupe en cause, si ces entrevues échappent à tout contrôle. Se sentant épiés par les autorités, les autres membres de ces groupes peuvent s'abstenir d'exercer leurs droits de désaccord légitime et permis par la loi. C'est un dilemme perpétuel pour le Service à qui on demande une attention soutenue et soigneuse chaque fois qu'un «événement spécial» se présente.

La production du renseignement

En vertu de l'article 12 de la *Loi sur le SCRS*, le Service a pour rôle principal de fournir des renseignements et des conseils au gouvernement. Nous nous sommes renseignés auprès

d'un certain nombre d'organismes fédéraux qui sont les principaux clients du renseignement d'AT et avons constaté qu'ils sont en général satisfaits de la qualité des renseignements qu'ils obtiennent sur les menaces terroristes. Ils déclarent également être en général satisfaits des consultations qu'ils peuvent avoir avec le personnel de l'AT pour discuter de questions et de problèmes. Les renseignements fournis aux clients sur la façon de découvrir des terroristes soupçonnés reçoivent un bon accueil, tout comme les analyses qui décrivent le degré de danger que présentent des organisations terroristes particulières à l'égard d'intérêts précis.

La divergence de vues entre le SCRS et les corps policiers face au terrorisme constitue un problème permanent. Le SCRS croit que les corps policiers voudraient, dans certains cas, que le Service utilise ses pouvoirs d'enquête pour soutenir le rôle des policiers, à savoir l'exécution de la loi. Mais ce n'est pas la raison d'être du SCRS. Ce Service a été créé principalement pour dispenser des conseils à partir d'analyses de l'information obtenue de sources ouvertes ou clandestines. Il est, bien sûr, de son devoir d'aider les corps policiers quand et où il le peut. Mais ce devoir porte avant tout sur la collecte de renseignements plutôt que sur le rassemblement d'éléments de preuve d'une manière qui puisse servir devant un tribunal. Le SCRS a terminé sa tâche quand il a cerné une menace et l'a indiquée aux policiers. Il ne devrait pas ensuite mettre en danger l'efficacité de ses méthodes afin de réunir des preuves qui pourront servir à porter des accusations et à obtenir des condamnations.

La coopération entre le SCRS et la GRC s'est grandement améliorée grâce, avant tout, aux échanges d'agents de liaison entre ces deux organismes. La divergence d'opinion sur l'importance à accorder au renseignement par opposition à la preuve continue à engendrer des tensions. L'insistance du SCRS à protéger ses sources amène parfois les corps policiers à se demander s'ils obtiennent toute l'information qu'ils souhaitent.

Au cours de notre examen, nous avons constaté que la Direction de l'AT donne son meilleur rendement lorsqu'elle s'occupe des menaces actuelles. C'est une direction opérationnelle et la plupart des renseignements qu'elle produit servent à des fins opérationnelles immédiates. Elle produit également des évaluations des tendances à long terme dans les pays qui ne présentent pas de menaces immédiates pour le Canada. Bien qu'il s'agisse probablement du produit le moins important, ces évaluations n'atteignent pas les normes des renseignements produits par la Direction de l'analyse et de la production, qui font l'objet du prochain chapitre.

Le même service qui exécute la recherche au sein de la Direction de l'AT s'occupe également des séances d'information à l'intention des cadres supérieurs, notamment du directeur du SCRS. Cette activité, aux échéances plus rapprochées, tend à bousculer celle du renseignement. Nous pensons qu'il sied bien que le directeur rencontre en personne d'autres éléments du monde du renseignement de sécurité et, naturellement, il doit être bien renseigné en vue de telles rencontres. Mais nous ne pensons pas que les séances d'information et la recherche opérationnelle fassent bon ménage dans l'organisation actuelle. Chacun joue un rôle important. Nous aimerions que ces rôles soient élargis et dissociés.

Si le directeur se promène, ce n'est pas le cas des analystes opérationnels de la Direction de l'AT. Ils n'ont pas souvent la possibilité d'assister à des réunions nationales ou internationales sur le terrorisme. Nous pensons qu'ils devraient avoir plus d'occasions de rencontrer

leurs homologues et leurs collègues des autres pays afin de mieux comprendre le travail de l'autre et, lorsque surviennent des événements qui prennent rapidement de l'ampleur, de disposer de relations personnelles et professionnelles qui permettent de faciliter le travail.

Conclusion

À la fin de notre étude, nous étions en général satisfaits des réponses que nous avons obtenues aux quatre questions posées au départ. Nous avons constaté que la Direction de l'AT protège les Canadiens comme il se doit. Elle respecte la loi. La *Loi sur le SCRS* offre un cadre convenable, distinguant le rôle du SCRS en matière de renseignement de celui de la GRC en matière d'exécution de la loi.

Par sa Direction de l'antiterrorisme, le SCRS prouve qu'il peut réunir de l'information de façon prospective, au delà de l'appui qu'il est tenu d'apporter à l'activité d'exécution de la loi.

Dans les secteurs où la Direction connaît des faiblesses depuis longtemps, comme celui de l'analyse, nous avons décelé une amélioration marquée. Le secteur où le besoin d'apporter d'autres améliorations se fait le plus sentir est celui de l'analyse stratégique à long terme, que nous abordons dans le prochain chapitre du présent rapport annuel.

6. De l'information au renseignement

L'information est la matière première que le SCRS transforme en produit fini : le renseignement, à savoir une information filtrée et présentée de manière à aider ceux qui s'en servent à prendre de bonnes décisions. Le SCRS comprend une Direction de l'analyse et de la production (DAP)* dont la tâche, selon le Manuel des opérations, consiste à évaluer les renseignements de concert avec les directions opérationnelles et à favoriser la transmission de l'information aux décideurs pertinents du gouvernement du Canada.

La DAP prépare des documents appelés *rapports du SCRS*, où sont résumés, dans chacun, des renseignements d'actualité sur un sujet, un organisme ou une personne unique, et des rapports spéciaux plus fouillés. Elle fournit également des documents et de l'information au Comité consultatif des renseignements (CCR) et au Comité consultatif de la sécurité (CCS). Il s'agit de sous-comités stratégiques du Comité interministériel de la sécurité et des renseignements (CISR) qui réunit des sous-ministres et qui relève du Comité du cabinet chargé de la sécurité et des renseignements, que préside le Premier ministre. Au total, cette Direction produit plus de 250 documents par année.

Nous avons procédé à un examen de l'activité d'analyse et de production de renseignements au sein de la DAP en 1987-1988. Comme le SCRS n'est pas seul à oeuvrer dans ce domaine, les ministères de la Défense nationale et des Affaires extérieures, pour ne citer que les exemples les plus flagrants, possèdent également leurs services d'envergure propres, et plusieurs organismes du gouvernement fédéral font usage de renseignements de sécurité : nos enquêtes nous ont inévitablement amenés à examiner les rapports qu'entretient le SCRS avec les autres organismes, à la fois producteurs et clients.

Dans le cadre de notre examen, le personnel de recherche a rencontré le personnel de tous les niveaux de la DAP : le directeur général, les chefs présents et antérieurs de sections et un certain nombre d'analystes. Nous avons assisté à toutes les étapes de la rédaction de certains projets de *rapports du SCRS*, examiné le travail exécuté par le CCR et observé les travaux du comité de production du renseignement de la DAP. Nous nous sommes également entretenus avec d'autres organismes qui ont recours aux renseignements du SCRS, nous avons étudié la formation, l'expérience et les titres universitaires des analystes de la DAP et consulté la documentation spécialisée pertinente. Nous nous sommes inspirés d'une enquête menée en 1987-1988 par la Direction elle-même sur sa clientèle.

Le rapport complet sera soumis à l'attention du Solliciteur général. Le présent chapitre en examine les constatations et les points fondamentaux.**

---

* Auparavant la Direction de l'évaluation des renseignements (DER).

** La DAP exerce également une fonction de surveillance sur les cibles antisubversives discrètes (voir chapitre 3 ci-dessus), mais notre étude s'est limitée à l'activité d'évaluation et de production comme telle.

Le renseignement

Nous avons fait nôtre la distinction apportée par le Groupe consultatif indépendant du Solliciteur général entre le renseignement opérationnel et le renseignement stratégique.* *Le renseignement opérationnel* est «lié aux enquêtes sur des activités considérées comme constituant une menace pour la sécurité du Canada. Il est recueilli surtout (mais non exclusivement) à l'aide de techniques d'enquête, sert à court terme, et est obtenu pour des clients bien précis ou à une fin particulière». Il s'agit d'un renseignement «axé sur le cas» et le SCRS en est lui-même à la fois le principal utilisateur et producteur. Le renseignement opérationnel est l'apanage des directions opérationnelles du SCRS, de l'Antiterrorisme et du Contre-espionnage, qui disposent de leurs propres analystes fonctionnels.

Le renseignement stratégique que produit la DAP «est davantage fondé sur la recherche à l'aide d'informations provenant de toutes les sources disponibles, vise une activité à plus long terme et de portée plus globale, et est destiné à un client interministériel ou au gouvernement dans son ensemble. Il est évalué à la lumière d'autres intérêts nationaux du Canada». À l'intérieur de cette catégorie, nous établissons une distinction entre le renseignement courant et le renseignement de base. *Le renseignement courant* porte sur des événements au fur et à mesure qu'ils se produisent et attire l'attention des décideurs sur les urgences éventuelles. *Le renseignement de base* est constitué de données fouillées sur des pays et des sujets, qui peuvent aider le gouvernement à élaborer ses politiques et à prendre des décisions stratégiques.

Prenons, à titre d'exemple, une réunion entre deux personnes soupçonnées de présenter une menace pour la sécurité du Canada : le renseignement opérationnel établirait la tenue de la rencontre et signalerait, dans la mesure du possible, ce qui s'y est dit. Le renseignement courant situerait la rencontre dans son contexte : déterminer à quelle organisation ces gens appartiennent, par exemple, et proposer ce que cette rencontre peut révéler des modifications susceptibles d'être apportées à l'intérieur de l'organisation et aux plans de cette dernière. Le renseignement de base offre un contexte plus vaste en évaluant les capacités, les intentions et les points vulnérables de l'organisation.

Le renseignement courant forme la majeure partie de la production de la DAP, comme le revèlent les observations faites par les clients selon lesquels *les rapports du SCRS* attirent leur attention sur les questions précises : la vente d'armes, par exemple. Nous y voyons une faiblesse; le gouvernement n'obtient pas tous les renseignements de base dont il a besoin. Un flot continu de rapports de renseignements courants peut amener à traiter le renseignement de sécurité comme une série de «questions brûlantes» plutôt que comme une activité permanente, à long terme.

Établissement des priorités

L'accent mis par la DAP sur le renseignement courant trouve en partie sa justification dans le SCRS lui-même. Cependant, ce n'est pas le SCRS mais le gouvernement qui

* *Des ressources humaines et un processus en transition*, pages 18 et 43.

détient l'ultime responsabilité d'arrêter les exigences et de fixer les priorités en matière de renseignement. Dans le monde occidental, une critique fort répandue dans le domaine du renseignement de sécurité porte sur le fait que les gouvernements ne donnent pas de directives suffisamment claires à leurs organismes de renseignement, et cette critique semble s'avérer dans le cas du Canada.

En l'absence de directives précises de la part du gouvernement, le SCRS a, incité par un certain nombre de facteurs, mis l'accent sur le renseignement courant. Les représentants du SCRS auxquels nous avons parlé nous ont cité, entre autres, l'inexpérience de la plupart du personnel de la DAP. Environ la moitié des analystes de cette Direction sont nouveaux dans le domaine du renseignement de sécurité étant donné que le SCRS n'a été créé qu'en 1984, et ils font leur apprentissage sur des projets à court terme de renseignements courants. Les analystes qui possèdent davantage d'expérience sont détournés de la production de renseignements de base en raison du temps qu'ils doivent consacrer à l'orientation de leurs subalternes. Cette situation, avons-nous appris, se modifiera au fur et à mesure que s'accroîtra le bagage d'expérience de la Direction.

Peut-être, mais il y a également des facteurs ancrés dans l'infrastructure. D'une part, la DAP ne possède pas de service consacré uniquement à la production de renseignements de base. L'influence des directions opérationnelles sur la DAP est beaucoup plus profonde.

Les directions opérationnelles, par l'entremise du comité de la production du renseignement (CPR) au sein du SCRS, jouent un rôle important dans l'établissement du programme de la DAP. Le Comité est présidé par le directeur général de la DAP, mais les directeurs généraux des directions opérationnelles détiennent la plupart des votes. Il existe un groupe supérieur «de direction» du CPR composé de sous-directeurs qui permettraient d'obtenir une perspective plus vaste, mais ce groupe est la plupart du temps inactif. Il ne s'est réuni qu'une fois en 1987. Le CPR de niveau des directeurs généraux (qui est le Comité dont nous voulons parler dans ce chapitre quand nous utilisons le sigle «CPR», à moins d'indication contraire) a tout naturellement comblé le vide.

Après avoir arrêté ce sur quoi l'attention des analystes de la DAP portera, le CPR entre en scène à nouveau à la fin de l'activité de production pour formuler ses observations sur le projet définitif de chaque rapport, exiger des révisions et décider de la distribution aux organismes et ministères-clients, aux agents de liaison de sécurité du SCRS à l'étranger et aux organismes de renseignement et de sécurité de pays étrangers amis.

Sources et méthodes

L'analyse repose sur un certain nombre de sources : l'information réunie par les directions opérationnelles dans le cadre d'enquêtes, les agents de liaison en matière de sécurité, l'information de sources ouvertes tels que les médias et les ouvrages publiés par les experts, les services de renseignement et de sécurité des pays amis et les autres membres du milieu canadien du renseignement.

Les directions opérationnelles continuent d'exercer leur influence une fois que le CPR a autorisé l'analyse d'un sujet. L'analyste de la DAP travaille souvent en étroite collaboration avec un homologue de la direction opérationnelle pertinente. La majeure partie de l'information brute utilisée par un analyste de la DAP provient de sources opérationnelles.

L'agent opérationel vérifie les conclusions de la DAP. Le document ainsi produit est parfois soumis à l'examen du directeur général de la direction opérationnelle avant même que le chef de l'analyste et le comité d'examen de la DAP en prenne connaissance.

Autre influence plus subtile, du moins dans un passé et un avenir immédiats, plusieurs des analystes de la DAP ont moins d'expérience et d'influence que leurs homologues des directions opérationnelles. De plus, la plupart des analystes de la DAP sont rattachés aux directions opérationnelles. Ils ont même leur bureau dans les locaux de ces directions auprès desquelles ils travaillent plutôt que d'être réunis, de sorte que la culture globale dans laquelle ils baignent est davantage opérationnelle qu'analytique. Dans une section, le bureau du chef est dans un autre immeuble que celui de la plupart des analystes qui relèvent de lui.

Nous étions heureux de constater que la Direction mise de plus en plus sur les sources ouvertes. Les lecteurs de nos rapports annuels constateront que le recours maximum aux sources ouvertes d'information constitue un des thèmes qui nous caractérisent (voir par. ex., page 21 du présent rapport). Notre consultation des données sur les clients pour 1986-1987 et 1987-1988 révèle une hausse de 10 pourcent des demandes de la DAP pour des données de sources ouvertes provenant du Centre d'information du SCRS.

Dans le passé (rapport annuel de 1986-1987, page 27), nous avons également eu l'occasion de souligner que le SCRS avait peut-être trop tendance à accepter d'emblée l'information fournie par les services de renseignement de pays amis. Nous avons appris, au cours de notre examen de la DAP, que les analystes portent un jugement critique sur l'information provenant de pays alliés où des questions particulières servent des intérêts personnels. De plus, la confirmation du renseignement provenant d'autres sources était un critère dans l'évaluation d'informations émanant d'autres services de renseignement; en théorie, on ne devrait pas accepter de telles informations tant qu'elles ne sont pas corroborées ailleurs.

Mais il n'est pas toujours facile d'obtenir cette confirmation, et les chefs de section de la DAP ne possèdent pas un accès suffisant aux terminaux informatiques qui leur permettraient de contrôler les documents de bases. Incidemment, cette situation et d'autres insuffisances sur le plan matériel ont peu d'importance mais révèlent le manque d'attention quotidienne de la part de l'administration supérieure à l'égard du travail de la Direction. Au cours de nos conversations avec des clients du renseignement, on a parfois fait allusion au fait que les *rapports du SCRS* n'ont pas toujours porté attention aux ramifications canadiennes. D'autres clients ont déclaré, cependant, que les efforts de la DAP visant à mettre davantage l'accent sur «les questions canadiennes» étaient évidents.

Quant aux méthodes d'analyse, la DAP n'a établi aucun modèle dont pourraient s'inspirer ses analystes. Le CCR et le CCS s'attendent à ce que le travail que l'on exécute pour eux soit présenté selon des dispositions particulières. Mais, en règle générale, la DAP compte sur chacun des analystes pour choisir la disposition qui convient au sujet traité. Nous ne proposons pas des méthodes rigides où les faits doivent être choisis au cadre plutôt que le cadre aux faits, mais nous nous inquiétons de l'absence de règles de base qui rend difficile l'évaluation du travail des analystes. Il faut trouver une solution médiane.

Les nouveaux analystes de la DAP doivent suivre un cours spécial donné par l'Académie Sir William Stephenson, école du Service, mais ce cours porte principalement sur l'analyse opérationnelle et ne comprend pas l'analyse politique et stratégique. Il s'agit d'une faiblesse à corriger le plus tôt possible. Les gestionnaires de la DAP s'entendent sur la nécessité de disposer d'une formation plus spécialisée en évaluation du renseignement et nous espérons que les pourparlers en cours aboutiront bientôt.

Spécialisation

Nous entretenons également certaines inquiétudes au sujet des obstacles qui, érigés au fil des ans au sein de la DAP, ont nui à l'acquisition de compétences spécialisées de calibre international. Au SCRS, on est majoritairement d'avis que les analystes doivent être des généralistes, non pas des spécialistes. Ce point de vue présente, à notre avis, certains avantages. Il permet à l'activité d'analyse de s'adapter plus rapidement aux priorités en évolution. Il favorise les idées neuves au fur et à mesure qu'une vaste gamme de connaissances et d'expériences entre en ligne de compte dans l'examen d'un sujet.

Mais la nécessité d'obtenir des connaissances approfondies dépasse de beaucoup, à notre avis, ces avantages. Les généralistes sont moins susceptibles d'être versés, par exemple, dans les cultures des groupes qu'ils étudient. Ils seront mal protégés contre les stéréotypes et moins capables de déceler des nuances importantes.

L'engouement pour la généralisation exprime plus qu'une question d'attitudes au sein du SCRS. Il a des racines administratives profondes qui se perpétueront indéfiniment à moins d'une décision nette et précise en faveur de la spécialisation.

Dans le barème de classification des emplois, les analystes se situent aux échelons AR-1 à AR-3 des employés qualifiés. Une fois l'échelon AR-3 atteint, ils pourraient avoir des difficultés à atteindre le niveau d'entrée dans les directions opérationnelles. Pour obtenir de l'avancement au sein de la DAP, ils doivent devenir gestionnaires plutôt que de demeurer analystes. Ainsi s'envole l'espoir d'une rémunération et d'une situation plus élevées qui motiveraient la tenue de l'étude indépendante que la spécialisation exigerait dans la situation actuelle. De plus, les échelons de la classification actuelle n'attireront vraisemblablement pas les spécialistes des autres directions ou de l'extérieur du Service.

Nous pensons qu'un échelon supérieur à AR-3 s'impose pour obtenir des analystes spécialisés supérieurs. À ce chapitre, nous pensons que la DAP pourrait être un bon endroit où placer certains des agents de liaison convenables du SCRS lorsqu'ils reviennent d'affectations à l'étranger. La production de renseignements pourrait tirer d'énormes avantages de leur vaste expérience. Mais comme ils détiennent des grades bien supérieurs à AR-3, la DAP n'est actuellement pas une destination qui les attire.

Deux autres contraintes administratives au chapitre de la spécialisation sont traitées dans un contexte plus vaste au chapitre 10; aussi, nous nous contenterons tout simplement de les mentionner ici. On incite les membres du SCRS à conserver l'anonymat; donc, ils présentent rarement des communiqués aux conférences. En fait, la Direction ne possède pas suffisamment de ressources pour même envoyer des analystes assister à des conférences.

(Cependant, le SCRS offre un programme interne de colloques et de communications réunissant des gens des autres secteurs du milieu, tant canadien qu'étranger, du renseignement de sécurité). Deuxièmement, il y a des empêchements statutaires aux mutations et aux détachements entre le SCRS et la Fonction publique.

Satisfaction des besoins du client

La tenue d'un sondage général auprès des clients en 1987-1988 témoigne favorablement de l'engagement pris par la gestion de la Direction afin d'améliorer son produit. Nous avons jugé qu'il s'agissait d'une démarche utile qui s'ajoutait à nos propres entrevues avec les clients. Le questionnaire destiné aux clients et remis avec chaque *rapport du SCRS* nous a laissé une moins bonne impression; les réponses qu'il sollicite sont superficielles. Nous nous préoccupons également de l'absence d'évaluation systématique, par la Direction, de son propre travail par l'examen des répercussions pratiques de chaque rapport.

Néanmoins, et malgré certaines critiques, le milieu du renseignement de sécurité semble s'entendre pour affirmer que les évaluations fournies par la DAP s'améliorent. Nous y avons relevé encore trop de descriptions et pas assez d'analyse, mais la DAP a manifestement déployé des efforts pour rétablir l'équilibre et mettre davantage l'accent sur la partie de la «portée canadienne» de ses rapports. La DAP reconnaît le bien-fondé des plaintes sur la nécessité de mieux justifier ses conclusions.

Les clients ont signalé les délais comme étant un problème; ils affirment ne pas recevoir suffisamment rapidement les *rapports du SCRS*. Par souci de rapidité, la distribution des rapports brefs et urgents se fait de façon électronique, mais le système présente une certaine lenteur. Le lourd mécanisme d'approbation des documents de la DAP serait en partie à blâmer. Au fur et à mesure que les analystes acquerront de l'expérience, il sera possible de les soustraire au comité d'examen composé de chefs de la DAP; chaque chef pourra assumer la responsabilité du travail de sa section et l'envoyer directement au CPR. Il faudra au moins fixer un mandat officiel au comité d'examen.

Le temps de traduction présente un autre problème. Il faut au moins une semaine pour faire traduire un document de 1 à 3 pages et ceux de plus de 20 pages exigent quatre semaines et plus. Pour accélérer le processus, la DAP pourrait adopter la pratique courante d'envoyer une première ébauche au service de traduction, de sorte que le document définitif ne présente que des révisions mineures. Cependant, comme dans tous les autres contextes, nous incitons également le SCRS à s'assurer qu'il dispose de suffisamment de traducteurs pour faire face aux exigences de la politique des langues officielles pour l'ensemble du gouvernement.

Certains clients ont déclaré que la cote SECRET attribuée aux *rapports du SCRS* en réduit l'utilité, puisqu'ils ne peuvent être remis, sans censure ou dispense spéciale, aux personnes qui pourraient en profiter mais qui ne possèdent pas l'habilitation de sécurité nécessaire. Certains clients ont également mentionné les liaisons au chapitre des problèmes. La DAP reconnaît la nécessité de renseigner directement des clients sur certaines questions qui présentent pour eux un intérêt particulier et de s'assurer que les répercussions du renseignement fourni sont bien définies et les besoins du client, bien compris.

Options éventuelles

Parmi nos principales constatations, mentionnons l'accent mis davantage sur le renseignement courant plutôt que sur le renseignement de base et, en l'absence de directives plus précises de la part du gouvernement, l'influence énorme des directions opérationnelles sur la DAP. Il existe un lien entre ces deux constatations. Les directions opérationnelles proposent les questions à analyser, en influencent la production au moyen des informations qu'elles fournissent et des examens officiels qu'elles exécutent, et décident en dernier ressort de ce qui sera divulgué.

Il faut que la direction du SCRS décide si elle souhaite conserver le statu quo, à savoir produire surtout du renseignement courant sous une forte influence opérationelle, ou doter la DAP des ressources et de l'organisation dont elle a besoin pour élaborer davantage du renseignement de base. Dans l'un ou l'autre cas, nous estimons que le CPR devrait, en proportion, être composé de moins de membres des directions opérationnelles et de davantage de membres de la DAP comme tel. Vu qu'elle est un service qui sert à l'ensemble du gouvernement, la DAP doit exercer davantage d'influence sur ses propres priorités en matière d'analyse et sur le contenu du renseignement qu'elle transmet.

La création d'un organisme d'évaluation distinct, selon le modèle australien, serait une autre option à envisager par le gouvernement pour produire du renseignement de base. Un tel organisme ne remplacerait pas la DAP, qui continuerait de produire du renseignement courant. Dans l'infrastructure canadienne actuelle, le chevauchement se ferait plutôt avec le CCR, dont le rôle est davantage de coordonner et d'autoriser que de produire des renseignements.

Au cours de notre visite en Australie, nous avons accordé une attention particulière au rôle de l'*Office of National Assessment (ONA)* indépendant qui s'y trouve. The Australian Security Intelligence Organization, (ASIO) correspond au SCRS au Canada. Il recueille, distribue des renseignements et les analyse, principalement du point de vue opérationnel. ONA est un évaluateur, pas un enquêteur, c'est un organisme externe pas interne, c'est à dire qu'il ne recueille pas de renseignements mais il s'en sert avec d'autres informations, dont certains de sources générales, pour publier des rapports, des appréciations et des évaluations. Il ne vise pas à la sécurité interne de l'Australie mais plutôt aux questions internationales, politiques, stratégiques et économiques qui touchent l'Australie.

Les représentants officiels de l'Australie sont convaincus de l'importance de l'évaluation indépendante du renseignement. Coupé des demandes urgentes des activités quotidiennes, tout en se tenant toutefois au courant, l'*ONA* peut se concentrer sur les besoins à long terme. On est alors moins tenté de consacrer des ressources aux travaux «orientés sur les données», c'est-à-dire, l'analyse de ce qu'ont révélé les enquêtes menées par les organismes d'enquêtes. Les études sont «orientées vers les besoins». Elles doivent viser un objectif précis et posséder au moins la possibilité d'aboutir à des recommandations en vue d'une mesure précise par le gouvernement. En fait, en sa qualité de membre à part entière du comité du secrétaire qui dessert le Cabinet et également grâce à ses évaluations des situations susceptibles de présenter des problèmes ou offrant trop peu de renseignements, l'*ONA* joue un rôle important dans l'établissement des priorités à mener par les organismes d'enquêtes, y compris le Department of Foreign Affairs and Trade, dont les rapports diplomatiques courants sont une source principale d'information pour l'ONA. Il joue le

rôle de critique institutionnel de la qualité et de la quantité d'informations que ces organismes fournissent.

Nous avons également été impressionnés par les compétences spécialisées auxquelles l'*ONA* a accès. La plupart des analystes de cet organisme possèdent des diplômes universitaires et ils font rarement partie du personnel pendant plus de cinq ans, de sorte que ce service bénéficie d'une arrivée constante de connaissances et de façons de penser des plus récentes provenant du monde des universitaires et des professionnels.

Nous tenons à préciser que nous ne recommandons pas, à ce stade-ci, d'imiter le modèle australien. Nous n'avons pas eu la possibilité d'examiner cette question plus en profondeur. Nous reconnaissons également les différences importantes qui existent entre le rôle de la DAP au sein du SCRS et le rôle de l'*ONA* en Australie. Nous croyons cependant qu'un organisme distinct est une option que le gouvernement pourrait envisager s'il partage notre point de vue face à la nécessité de plus de renseignements de base.

Résumé

Avant la création du SCRS en 1984, l'histoire des services d'évaluation en matière de renseignement canadien de sécurité démontrait des échecs dès leur mise sur pied. La situation a changé. Nous avons constaté que la DAP devient davantage un service qui produit le genre de renseignement dont le CSARS estime que le gouvernement a besoin.

Les gestionnaires de la Direction ont pris d'importantes initiatives pour que leur produit devienne le meilleur qui soit, compte tenu des circonstances. Nous avons cité le sondage auprès des clients, qui a été bien exécuté. Les directions opérationnelles ont signé des protocoles d'entente prévoyant un partage bien délimité des responsabilités. La DAP s'est acquis le respect des directions opérationnelles et, ainsi, l'accès qui lui était essentiel aux renseignements délicats détenus par ces directions.

Cependant, la DAP ne peut faire toute seule que certains progrès. En particulier, les politiques en matière de personnel à l'échelle du service empêchent l'embauche et le perfectionnement de spécialistes possédant une connaissance approfondie des antécédents sociaux et culturels des cibles du SCRS. L'engagement de principe incontesté pris par la direction du Service à l'égard de l'analyse et de la production ne semble pas être respecté dans le quotidien.

Nous sommes d'avis que le Canada obtiendra le meilleur renseignement stratégique possible quand la DAP rehaussera son groupe de professionnels qui seront acharnés à produire des analyses axées sur la politique en faisant appel à toute une gamme d'informations dont dispose le gouvernement, plutôt qu'en se basant sur le produit fourni par les enquêtes sur place. Si pareil groupe ne convient pas au SCRS, le gouvernement pourrait songer à en créer un ailleurs.

7. Plaintes

Comme nous l'avons déjà expliqué, notre mandat en vertu de la *Loi sur le SCRS* est double : le contrôle et les plaintes. Le paragraphe 38c) de la *Loi* nous oblige à faire enquête sur les plaintes que peut formuler toute personne au sujet des activités du Service et de plaintes au sujet du refus d'habilitation de sécurité au chapitre de l'emploi dans la Fonction publique, de la fourniture de biens et de services au gouvernement du Canada et de questions d'immigration et de citoyenneté, ainsi que de faire enquête sur les questions de sécurité liées à certaines plaintes déposées devant la Commission canadienne des droits de la personne.

L'annexe B du présent rapport donne un résumé des plaintes qui ont fait l'objet d'une enquête en 1987-1988. Le présent chapitre brosse une vue d'ensemble et traite des questions de l'heure à ce sujet.

Les plaintes en 1987-1988

En 1987-1988, nous avons reçu 38 nouvelles plaintes, soit exactement le double du chiffre de l'année précédente (voir le tableau 3 ci-après). Le nombre des plaintes au sujet du refus d'habilitations de sécurité et au sujet de questions de sécurité en matière d'immigration est demeuré le même qu'en 1986-1987, soit 1 et 2 dans chacun des cas. Quant au nombre de plaintes au sujet de l'intention de refuser la citoyenneté pour des motifs de sécurité nationale ou de participation à des activités de crime organisé, il est passé à 1 en 1987-1988, comparativement à 2 l'année précédente.

Par contre, le coefficient de la hausse des plaintes formulées en vertu de l'article 41 de la *Loi* se situait à 2,6. En vertu de cet article, «toute personne peut porter plainte contre des activités du Service». Nous devons faire enquête si trois conditions sont réunies : premièrement, le directeur du SCRS doit avoir la possibilité d'y répondre et, deuxièmement, nous devons nous assurer que la plainte n'est pas «frivole, vexatoire, sans objet ou entachée de mauvaise foi» et, finalement, qu'il n'existe aucune autre possibilité de recours en vertu soit de la *Loi sur le SCRS*, soit de la *Loi sur les relations de travail dans la Fonction publique*. En 1987-1988, le nombre de ces plaintes se chiffrait à 34 comparativement à 13 l'année précédente.* De ce nombre, il y avait également deux affaires reportées de l'année 1986-1987.

La nature des plaintes formulées en vertu de l'article 41 ne présentait aucune constante. La hausse s'explique simplement par une sensibilisation accrue du public à l'égard de notre Comité et de ses travaux plutôt que d'une faiblesse particulière du SCRS. Le règlement de 30 plaintes a pu se faire rapidement; il s'agissait d'affaires qui ne relevaient manifestement pas de notre compétence ou de plaignants dont la cause n'était pas fondée sur des faits permettant de mener une enquête. Nous avons fait enquête au sujet de deux plaintes. Dans ni l'une ni l'autre, nous n'avons pu constater d'erreur de la part du SCRS.

---

* Ce chiffre ne tient pas compte des plus de 2 000 plaintes formulées par des employés du SCRS en 1985-1986 et en 1986-1987 au sujet des pratiques du Service en matière de langues officielles. Ces plaintes ont fait l'objet d'une enquête spéciale que nous avons publiée en 1986-1987 sous le titre *Pour corriger une situation*.

Au sujet d'une plainte visant une habilitation de sécurité, nous avons recommandé d'accorder l'habilitation. Il est trop tôt pour affirmer si notre recommandation sera suivie. Dans les affaires de citoyenneté, trois dossiers ont été clos avant que nous ayons terminé notre enquête parce que le SCRS a retiré l'opposition qu'il avait formulée. Dans la quatrième affaire, nous avons convenu que la citoyenneté devait être refusée. Au chapitre de l'immigration, nous avons convenu de l'expulsion d'une personne et, dans la deuxième affaire, où la criminalité était en cause, le dossier a été clos avant que prenne fin l'enquête parce que la GRC a retiré son opposition à l'entrée de la personne au Canada.

Comme l'illustre le tableau 3, en 1987-1988, nous avons terminé l'étude de 39 plaintes. Des 14 dossiers reportés de l'année précédente et des 38 nouvelles plaintes, il ne nous restait, à la fin de l'année, que 13 dossiers à régler, soit un chiffre acceptable puisqu'il est inférieur de 1 à celui de l'année dernière à la même époque.

Tableau 3. Bilan des plaintes, 1987-1988

	Nouvelles	Reportées de 1986-87	Réglées	Reportées à 1988-89
Habilitations de sécurité	1	1	1	1
Citoyenneté	1	7	4	4
Immigration	2	4	2	4
Article 41	34	2	32	4
Total	38	14	39	13

Qui décide?

En 1987-1988, une question d'une grande importance à long terme a finalement connu un dénouement lorsque la Cour fédérale d'appel a arrêté comme *Obiter Dicta* dans l'affaire *Thomson c. La Reine* que les sous-ministres étaient tenus de respecter nos recommandations en matière d'habilitation de sécurité en vue d'un emploi dans la Fonction publique; lorsque, après enquête, nous arrivons à la conclusion que l'habilitation a été refusée sans raison, le sous-ministre en cause doit acquiescer à notre recommandation d'accorder ladite habilitation.* Le tribunal a déclaré que le maintien de refus pourrait se justifier par de nouveaux renseignements obtenus après la fin de notre enquête. Un tel refus pourrait, certes, donner lieu à une nouvelle plainte que nous aurions à trancher.

Cependant, personne ne s'attendait à ce que cet arrêt règlât définitivement la question. C'est ce qui est arrivé. Pour des raisons juridiques, la même affaire a abouti devant la Division de première instance de la Cour fédérale en vue d'une décision peu de temps après et l'arrêt de ce dernier tribunal a infirmé celui du premier; les sous-ministres ne sont pas

* Arrêt non publié rendu par la Cour fédérale d'appel le 7 mars 1988.

tenus de suivre nos recommandations, a déclaré le juge Dubé de la division de première instance.* Cette décision fait actuellement l'objet d'un appel.

Voici comment est née cette affaire. M. Robert Thomson a réussi un concours en vue d'un poste au ministère de l'Agriculture. Le poste exige l'habilitation de sécurité de niveau SECRET (devenu le niveau II), sa nomination était donc liée à l'obtention de cette habilitation. Après enquête menée à la demande du Ministère, le SCRS recommandait de refuser l'habilitation. Figurent au dossier un certain nombre de soupçons à l'endroit de M. Thomson, dont la «fuite» d'au moins un document qu'il aurait eu en sa possession quand il travaillait à l'Agence canadienne de développement international il y a quelques années. Après avoir consulté les fonctionnaires de son ministère et du bureau du Conseil privé, le sous-ministre refusa l'habilitation et l'offre d'emploi fut retirée.

M. Thomson nous adressa alors une plainte. Conformément à notre façon habituelle de procéder, deux d'entre nous ont fait enquête. M. Thomson, le Ministère et le SCRS étaient tous représentés par un avocat. On en arriva à la conclusion que M. Thomson «ne divulguerait vraisemblablement pas de renseignements cotés s'il occupait à nouveau un poste lui donnant accès à de tels documents». Nous avons recommandé d'accorder à M. Thomson la cote SECRET afin qu'il puisse accepter le poste. Le sous-ministre est demeuré inflexible dans sa décision originale et M. Thomson a intenté une demande de réparation devant la Cour fédérale d'appel.

C'est à ce moment que la Cour d'appel a déclaré que le sous-ministre n'avait pas d'autre choix à ce chapitre : il devait respecter notre recommandation. Cependant, le tribunal n'avait pas compétence pour infirmer la décision du sous-ministre puisque des questions semblables sont l'apanage de la Division de première instance. M. Thomson s'est donc adressé à cette Division pour obtenir l'arrêt du juge Dubé.

Tant que les Cours n'auront pas statué sur ce cas, il ne serait pas convenable que nous portions un jugement sur le bien fondé de ces points juridiques.

Communication

La communication de renseignements au plaignant soulève une controverse constante entre le Comité et le SCRS. Tout en reconnaissant la responsabilité du Service à l'égard de la protection de la sécurité nationale, nous hésitons toujours à passer outre à son avis et à communiquer au plaignant des renseignements. Mais nous avons l'obligation de nous assurer que le plaignant possède suffisamment de renseignements pour se défendre de façon éclairée contre les soupçons qui pèsent sur lui.

L'article 46 de la *Loi sur le SCRS* définit cette obligation face au refus d'une habilitation de sécurité en vue d'un emploi au gouvernement ou d'un marché de l'État. Il affirme que

* Arrêt non publié rendu par la Division de première instance de la Cour fédérale d'appel du Canada le 15 juin 1988. Cette décision fut rendue après la fin de l'année visée par le présent rapport, mais nous avons jugé nécessaire de la mentionner ici; autrement cette image ne refléterait pas la réalité.

nous devons donner au plaignant «un résumé *des informations dont [le comité] dispose à ce sujet* afin de permettre au plaignant d'être informé *de la façon la plus complète possible* des circonstances qui ont donné lieu au refus d'une habilitation de sécurité». En principe, le plaignant doit détenir toutes les informations pertinentes dont nous disposons, sous réserve de la mesure du «possible». La principale limite que nous admettons dans la communication de renseignements au plaignant est la protection obligatoire des sources du SCRS. Il existe des dispositions semblables au sujet des plaintes en matière de citoyenneté et d'immigration.

Nous avons appris que, en Australie et en Nouvelle-Zélande, la communication ne présente pas de difficulté. Le président de *Australia's Security Appeals Tribunal* a déclaré que l'*Australian Security Intelligence Organization*, qui est le pendant du SCRS au Canada, collabore en général pour communiquer au plaignant suffisamment de renseignements pour lui permettre de bien se défendre. En Nouvelle-Zélande, sir Thaddeus Pearcey McCarthy, *Commissionner of Security Appeals*, nous a déclaré qu'il a toujours donné au plaignant tous les détails des soupçons révélés par les sources camouflées.

Ici, au Canada, nous avons constaté que le SCRS fait preuve d'une prudence exagérée dans ce qu'il estime pouvoir communiquer au plaignant et nous avons dû souvent adopter une attitude intransigeante. Le SCRS continue à penser que ce processus est déroutant. Dans une affaire, le SCRS a retiré son opposition à l'octroi de la citoyenneté à une personne plutôt que de nous permettre de divulguer les renseignements dont la personne, estimions-nous, avait besoin pour se préparer une défense valable.

8. Au CSARS

Les chapitres antérieurs décrivent nos activités en matière de contrôle et de plaintes. Les chapitres à venir portent sur deux sujets généraux qui font partie de notre menu quotidien : notre travail visant à favoriser un débat public éclairé des questions de sécurité et de renseignement et, deuxièmement, certaines questions que le Parlement et les Canadiens souhaitent examiner au moment de la révision de la *Loi sur le SCRS* en 1989. Le présent chapitre étale certains détails administratifs.

Notre travail de membres du CSARS

C'est, bien sûr, notre personnel qui exécute la plupart des travaux quotidiens de notre Comité et la plupart des travaux de recherche. Mais nous prenons tous une part active personnelle à l'exercice du contrôle et à l'étude des plaintes. Nous nous réunissons en comité au moins une fois par mois pour débattre des questions et prendre des décisions stratégiques. Chacun de nous travaille, avec l'aide du personnel, à certains projets comme l'étude sur l'antiterrorisme sur laquelle porte le chapitre 5. Nous faisons, en personne, l'audition des plaintes, mais avec l'aide d'un comité d'audition d'un ou deux membres désignés par le Président pour répartir le travail.

Nous continuons de croire à la valeur d'un comité comme le nôtre, qui se réunit à temps partiel et qui regroupe des représentants de tous les partis politiques, pour exercer le contrôle et faire enquête au sujet des plaintes. Le mécanisme tripartite de nos nominations en vertu de la *Loi* garantit au Parlement et au public notre impartialité. Cette situation n'a pas encore empêché l'emploi d'une méthode collégiale dans l'exécution de nos travaux. Le fait que nous ne soyons pas des fonctionnaires permanents présente également une certaine valeur. En continuant d'être des membres actifs de nos collectivités des différentes parties du pays, nous pouvons conserver le dégré de détachement qui convient à un organisme de contrôle.

Rapport financier

Nos dépenses pour 1987-1988 figurent au tableau 4.

Tableau 4. Budget du CSARS, 1987-1988

Personnel		$565,000
Traitements et salaires	$491,000	
Contributions aux régimes d'avantages sociaux des employés	$74,000	
Biens et services		$661,000
Services professionnels et spéciaux	$507,000	
Autres	$154,000	
Total des dépenses de fonctionnement		$1,226,000
Dépenses de capital		$9,000
TOTAL		$1,235,000

(Source : Budget des dépenses pour 1988-1989, Partie III)

Personnel

Nos effectifs se chiffrent toujours à 13, à la tête desquels se trouve un secrétaire exécutif qui dirige toutes les activités quotidiennes. Nos autres employés comprennent un directeur de la recherche, deux recherchistes et une adjointe de recherche, un agent principal chargé des plaintes, une adjointe exécutive qui remplit des fonctions relatives à la recherche et aux plaintes, un agent administratif qui est également le greffier de nos audiences et le coordonnateur des requêtes en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*, un agent des documents, un commis aux documents et trois secrétaires.

9. Besoin de savoir

Le *besoin de savoir* est une des expressions les plus usitées dans le domaine de la sécurité et du renseignement. Au sein du SCRS et chez les organismes semblables dans le monde entier, l'information est communiquée selon le besoin de savoir. Chaque fait, chaque idée n'est confiée qu'à ceux qui en ont besoin pour exécuter leur travail. Tous les autres sont laissés dans l'ignorance. Le danger de fuite est ainsi diminué et la liste des suspects est limitée, si fuite il y a.

Il existe un autre besoin de savoir : celui du public au sujet de ce qui se fait en son nom. Maints détails du travail en matière de sécurité et de renseignement doivent, bien sûr, demeurer secrets pour des raisons manifestes : toute publicité avantagerait les adversaires de la démocratie. Mais on peut divulguer bien des choses sans mettre en péril la sécurité nationale, et il faut le faire.

Annuaires des services de renseignement et de sécurité

Comme nous l'avons déjà signalé l'an passé, lorsque nous avons assumé nos fonctions de membres attitrés du CSARS, nous nous sommes rendus compte qu'il n'était pas possible de consulter rapidement certaines informations fort simples. Par exemple, comme nouvel arrivant dans le monde du renseignement nous désirions trouver un annuaire complet des organismes fédéraux qui s'adonnent à des activités de sécurité et de renseignement.

Grâce à la collaboration généreuse de tous les intervenants, nous avons dressé nous mêmes un annuaire complet qui se révèle très utile pour les nouveaux arrivants y compris les nouvelles recrues du SCRS.

Nous avons donc préparé une version expurgée destinée à la consommation publique et l'avons publiée à titre d'annexe C du présent rapport. Nous tenons à faire une mise en garde : il s'agit d'un ouvrage purement descriptif; il ne renferme rien qui pourrait être considéré comme l'évaluation des divers organismes qu'il décrit.

Sensibilisation

L'annuaire constitue un exemple d'effort concret visant à sensibiliser davantage le public aux questions de renseignement de sécurité et à mieux faire connaître le travail du SCRS. Le rapport annuel est notre principal moyen. Sa préparation vise principalement à satisfaire à une obligation prévue dans la loi, bien sûr, mais nous sommes également conscients du rôle qu'il peut jouer dans l'information du Parlement, du monde universitaire et d'autres spécialistes, des médias et (surtout par l'entremise des médias) du peuple canadien. En l'absence de toute autre source ouverte, le rapport offre les seules statistiques dont disposent les Canadiens en général au sujet des mandats accordés au SCRS. Il nous a permis de poursuivre le débat sur des dossiers tels que l'emploi de sources ouvertes et les méthodes de ciblage.

Le rapport annuel constitue le document de base pour ceux qui doivent se présenter devant les comités parlementaires. Au cours de l'année à l'étude, nous avons comparu le 17 décembre 1987 devant le Comité permanent (de la Chambre des communes) de la Justice et du Solliciteur général (et une seconde fois, le 14 avril 1988, peu après la fin de l'exercice financier).

Comme l'explique le chapitre 2, nous avons également remis des rapports spéciaux au Solliciteur général, dont certains ont été rendus publics. En mars 1988, nous avons publié notre rapport spécial sur l'usage par le SCRS de ses pouvoirs d'enquête en ce qui concerne le mouvement ouvrier (voir le chapitre 3 pour un examen des principales constatations). L'an dernier, nous avons publié : *Pour corriger une situation*, un résumé de notre rapport au Solliciteur général sur les pratiques en matière de langues officielles et les relations de travail au sein du Service.

Un autre moyen important de renseigner le public se trouve dans les invitations que nous acceptons afin de prendre la parole devant des publics intéressés. Le président, Ronald G. Atkey, a prononcé le 8 mai 1987 une allocution sur la responsabilité en matière d'activité de renseignement de sécurité au Canada, à l'occasion d'une conférence tenue par l'*Osgoode Hall Law School* et intitulée : *Domestic Security : Issues for Democracy*.

Jean-Jacques Blais a pris la parole devant des étudiants en sciences politiques de l'Université Carleton à Ottawa, l'automne dernier, tandis que Paule Gauthier a brossé un tableau du travail de notre Comité dans le cadre d'une allocution devant l'Association des femmes juristes du gouvernement fédéral en janvier 1988 et a pris la parole devant la faculté de sciences politiques de l'Université Laval à Québec le printemps dernier. Vers la fin de l'année, M. Blais se préparait à prononcer une allocution sur la responsabilité politique des services de renseignement au Canada à la conférence de 1988 de la *Canadian Association for Security and Intelligence Studies*.

Nous entretenons des rapports fréquents avec les médias qui se tournent vers nous pour obtenir des renseignements et de la documentation lorsque font surface des nouvelles portant sur le renseignement de sécurité. Nous avons tenu une conférence de presse au moment du dépôt de notre dernier rapport annuel en juin 1987.

Recherche académique canadienne

Nous nous sommes également préoccupés de satisfaire le besoin constaté en matière de recherches académiques dans les domaines du renseignement de sécurité au Canada. La majorité des connaissances et des idées que nous possédons sur ces sujets au Canada proviennent de l'étude de l'expérience européenne ou américaine.

Dès 1985, afin de nous préparer à nos responsabilités de mise sur pied du CSARS, nous avons tenu un colloque réunissant environ deux douzaines d'universitaires appartenant à des disciplines pertinentes, ainsi que d'autres spécialistes, qui nous ont fait part de leurs connaissances et de leurs points de vue. Certains des sujets abordés alors sont toujours au coeur de nos méthodes : notre préoccupation d'établir un équilibre entre la protection des libertés fondamentales et le rassemblement de renseignements efficaces.

Cette année, nous avons participé à la tenue de deux conférences. Celle de l'*Osgoode Hall Law School* à l'Université York, les 8 et 9 mai 1987, intitulée «*Domestic Security : Issues for Democracy*» , dont nous avons partagé la présentation avec le *School's Centre for Public Law and Public Policy*. Puis, nous avons partagé avec l'inspecteur général la présentation d'une conférence intitulée «La défense d'une cause, la protestation et la manifestation d'un désaccord» à l'Université Queen's à Kingston, du 25 au 27 février 1988. Point n'est nécessaire de s'arrêter ici sur les comptes rendus de ces conférences, car ils seront

bientôt publiés, sauf pour signaler qu'elles constituent un pas important vers l'objectif d'un débat éclairé.

Un membre de notre équipe de recherche, a présenté une communication à un colloque international tenu à l'Université de Séville, en Espagne, du 25 au 27 février 1988.*

Il dispute de l'idée selon laquelle, sans l'attention des médias, le terrorisme dépérirait. Ainsi, lorsque les autorités cèdent aux pressions afin de sauver des vies innocentes, parfois au prix d'une publicité internationale négative, les terroristes voient leur conviction confirmée que la violence donne des résultats. L'établissement de liens à l'intérieur de la cellule terroriste et la réputation de «héros» dont jouit le terroriste auprès des sympathisants contribuent également à alimenter ce phénomène.

Mais la modification du comportement des cibles immédiates au moyen de l'agression et de la violence est rarement l'objectif global du terroriste. En recherchant l'attention des médias, il vise à diffuser sa propagande, à démoraliser le public et les autorités, par exemple, ou à attirer de nouveaux sympathisants et à intéresser des recrues éventuelles.

Médias : Amis, adversaires . . . ou les deux?

Manifestement, les médias jouent un rôle primordial dans la montée et l'ampleur actuelles du terrorisme et dans la façon dont sont commis des actes individuels de terrorisme. En général, les médias exercent une force positive dans la promotion d'un débat éclairé sur des questions de sécurité et de renseignement. Il n'existe pas, dans la société, d'autres organismes ayant une portée et une capacité de présenter des questions de façon compréhensible pour la plupart des gens. Nous n'ignorons cependant pas les problèmes que peuvent susciter les reportages sur le terrorisme et sur le renseignement de sécurité en général. Dans le chapitre introductif du présent rapport, nous avons souligné l'atmosphère de doute qui régnait dans les médias canadiens à l'affût de certains problèmes réels du SCRS, qui ont donné lieu à certains reportages douteux. Et quand les terroristes marquent des points tout simplement en faisant les manchettes, alors les reportages sur les terroristes sont comme une bombe à retardement.

Certains cas de conflit, survenus au Canada, entre le droit du public de connaître qui est servi par le média et les exigences légitimes en matière de sécurité ont fait l'objet de documents déposés devant le Comité du Sénat sur le terrorisme et la sécurité publique.** Les cas à l'étranger sont bien connus, le «syndrome de Beyrouth», par exemple, où les grands médias accèdent aux conditions des terroristes de diffuser l'information.

---

* M. Klein, *Terrorism and the Media : A Social Learning Approach*, document présenté au *Ninth International Colloquium on the Brain and Aggression*, Université de Séville, du 25 au 27 février 1988. Les idées exprimées dans le document sont celles de l'auteur, non pas nécessairement celles du comité; mais nous souscrivons aux idées exprimées dans le présent rapport.

** Sénat du Canada, *Rapport du Comité spécial du Sénat sur le terrorisme et la sécurité publique*, Ottawa, Approvisionnements et Services Canada, 1987.

Il est utopique de s'attendre à ce que les médias arrêtent de faire des reportages sur le terrorisme. Ce n'est pas souhaitable, car le public a besoin de savoir comment se joue le jeu de la politique, si les moyens sont honnêtes ou si les dés sont pipés. Mais nous souscrivons sans hésitation à l'observation formulée dans *Terrorism and the Media : A Social Learning Approach*, selon le rapport il importe que les journalistes soient suffisamment éclairés pour se rendre compte quand et comment ils se font manipuler par les mouvements terroristes. Parfois il s'agit simplement d'une question de moment opportun : le public a-t-il besoin d'obtenir un rapport direct à vous couper le souffle dès le moment où le groupe d'intervention prend position ou peut-il attendre quelques heures? Parfois il s'agit d'une question compliquée : les journalistes devraient-ils accepter le rôle, comme certains journalistes irlandais, de mener une propagande terroriste sans critique dans l'espoir d'obtenir en retour des bribes d'informations exclusives?

Porte-parole du SCRS?

Le besoin d'avoir une image réaliste du SCRS constitue un autre aspect du besoin de savoir du public. Nous assumons certaines responsabilités. Notre adjointe exécutive, a insisté sur le réalisme lorsqu'elle a pris la parole devant le Centre pour le journalisme d'enquête à l'occasion de la 10e conférence annuelle tenue à Toronto les 25 et 26 mars 1988. James Bond est un personnage amusant, mais qui fait partie de la fiction, a-t-elle affirmé. On rendrait un plus grand service à la vérité si l'on transformait l'image de l'espion vêtu d'une cape noire et armé d'un poignard par celui d'une machine à écrire et de quelques fiches.

Le SCRS lui-même assume, bien sûr, une certaine responsabilité. Nous l'avons déjà invité (rapport annuel de 1986-1987, page 53) à entamer une campagne de relations publiques destinée à sensibiliser les Canadiens à son rôle. À notre avis, cela aurait un effet marqué sur les relations de travail et donnerait aux employés une image de marque positive qui appuierait leur propre croyance à une contribution personnelle à la sécurité du Canada. Puis on atteindrait également l'objectif d'information du public.

Nous avons applaudi tout particulièrement aux efforts déployés récemment par le Solliciteur général afin de sensibiliser davantage le public et de lui faire connaître le travail inestimable qu'exécute le SCRS. Prenant la parole le 21 avril 1988 devant le *Confederation Club* à Kitchener, il a, par exemple, déclaré que suite aux renseignements fournis par le SCRS, plus d'une douzaine de diplomates étrangers sont rentrés dans leur pays après que leurs activités d'espionnage aient été mises au jour et plusieurs autres ont été déclarés *persona non grata* en permanence.* Le 5 mai 1988, en prenant la parole au Kiwanis Club de Vancouver, il a déclaré que le SCRS avait traité 50,000 vérifications de sécurité pour les Jeux Olympiques et qu'aucun terroriste avait réussi à s'infiltrer. Voilà encore de l'information que les Canadiens devraient connaître.

* À la fin de l'exercice à l'étude, en juin 1988, un autre exemple de ce genre d'activité a été rendu public. Nous avons été mis au courant et nous ferons des observations dans le prochain rapport annuel.

10. Cinq ans après

Au cours des récentes années le Parlement a prévu que certaines des lois qu'il passe seront revisées dans un certain délai. L'article 69 de la *Loi sur le SCRS* pourrait être qualifiée de vedette, prévoit «un examen complet des dispositions et de l'application de la Loi», par un comité désigné ou constitué par le Parlement, en 1989, cinq ans après son entrée en vigueur.

Dans une démocratie telle que la nôtre, les délibérations du Parlement ne se font pas sans travail de recherche préalable. Derrière les débats de 1983 et de 1984 se trouvent les travaux de la Commission McDonald qui ont duré de 1977 à 1981 et un débat public qui remonte aussi loin qu'à 1960. Au moment où les feux du Parlement s'orientent à nouveau sur la *Loi*, le public a voix au chapitre. Les spécialistes feront connaître leurs points de vue, ainsi que d'autres qui détiennent un intérêt personnel ou professionnel dans le renseignement de sécurité. Les médias nous feront connaître divers points de vue et, probablement, certains des leurs.

Nous avons également l'intention de jouer un rôle dans ce débat. En notre qualité de surveillants du SCRS depuis sa création, grâce à l'accès total à ses dossiers et grâce à notre situation de service supplémentaire qui nous permet de parler franchement dans les limites imposées par les questions de sécurité nationale, nous nous estimons tenus de partager ce que nous avons appris. Nous avons déjà formulé certaines propositions dans les rapports annuels des années passées. En vue de 1989, nous formulerons des propositions particulières de modifications dans le rapport annuel de l'an prochain.

Mais le Parlement et le public ne souhaiteraient pas entamer de but en blanc cette activité d'examen. Par conséquent, oubliant pour un instant les questions internes, nous avons consacré le présent chapitre à certaines des questions que nous avons relevées. En générale nous les présentons sous forme interrogative parce que nous ne voulons pas écarter toute option.

Le renseignement de sécurité et la politique publique

Le rassemblement de l'information et sa transformation en renseignement visent à servir des intérêts à long terme du Canada en matière de stratégies et de politiques. On n'a pu y arriver que par une communication constante entre ceux qui élaborent les politiques et ceux qui produisent les renseignements. Maints auteurs ont fait remarquer, sans viser particulièrement le Canada, mais plutôt afin de soulever une tendance générale dans le monde occidental, que les utilisateurs de renseignement ne savent souvent pas ce qu'ils peuvent obtenir ou ce qui peut être produit, tandis que, par contre, ceux qui les produisent ne savent souvent pas au sujet de quelles questions les décideurs ont besoin de renseignements.

Au Canada, les utilisateurs de renseignements sont aussi nombreux que les services de l'État. Ils comprennent les ministères et les hauts fonctionnaires de tous les ministères et organismes. Il y a également tous ceux qui produisent diverses sortes de renseignements (voir l'annexe C du présent rapport) : les renseignements économiques, étrangers, militaires et les renseignements de sécurité. Le SCRS n'est qu'un des participants.

Un autre aspect de la question est lié aux excellentes relations que le SCRS entretient, heureusement, avec les organisations soeurs des pays amis. Comme le Canada partage les

intérêts de ces pays, les renseignements que le SCRS en obtient sont d'une grande utilité pour les clients canadiens. Cependant, nous avons parfois soupçonné le SCRS d'adopter trop rapidement le point de vue de ces organismes au détriment des priorités canadiennes.

Au chapitre 6, nous avons mentionné l'expérience de l'Australie au sujet de l'*Office of National Assessment* qui est un organisme distinct de ceux qui réunissent des renseignements étrangers et intérieurs.

> *Faudra-t-il instaurer un nouveau mécanisme chargé de réunir des renseignements de toutes sortes avant de les communiquer à ceux qui rédigent les politiques et prennent les décisions?*

Le renseignement de sécurité et la communauté canadienne

Partout dans le monde, les services de renseignement de sécurité vivent un certain isolement du reste de la société. Pour des motifs de sécurité nationale, un service de ce genre ne peut pas échanger ouvertement des renseignements avec le secteur privé, les hommes politiques, les enseignants, les médias d'information, voire même les autres services de l'État.

La situation est fort différente dans d'autres secteurs du gouvernement. Plusieurs fonctionnaires ont poursuivi des carrières réussies dans le monde des affaires, des professions libérales, des organisations sans but lucratif, des syndicats, des médias ou de tout autre secteur possible. Les travaux spécialisés sont adjugés à des spécialistes de l'extérieur. Il y a des mutations de personnel entre les ministères et les organismes. Les fonctionnaires assistent à des conférences où ils échangent points de vue et informations avec des personnes du secteur privé et du bénévolat. De cette manière et de bien d'autres façons, les fonctionnaires demeurent intégrés à l'ensemble de la société et ont la possibilité de se tenir au courant des progrès qui s'y font.

Par ailleurs, les agents de renseignement de sécurité débutent habituellement dans ce domaine à un âge assez jeune et y demeurent jusqu'au moment de leur retraite. Au Canada, les agents du SCRS ne sont pas régis par la *Loi sur l'emploi dans la Fonction publique*, n'étant donc pas des «fonctionnaires» au sens juridique strict du terme. Donc, pour toutes sortes de raisons pratiques, il est quasi impossible d'obtenir de mutations entre le SCRS et d'autres services du gouvernement fédéral. Les agents du SCRS souhaitent conserver l'anonymat et évitent les endroits tels que les conférences où la nature de leur travail pourrait être dévoilée. Pour toutes ces raisons, le SCRS s'interdit nombre de possibilités d'échange qui pourraient être enrichissantes.

> *Devrait-on modifier la loi pour faciliter les mutations entre le SCRS et les autres services du gouvernement fédéral?*
>
> *Vaudrait-il la peine de mener une enquête poussée requise pour le triage sécuritaire pour permettre à des spécialistes de l'extérieur d'être mutés au SCRS?*

La communication de renseignements

L'article 19 de la *Loi* régit la communication de renseignements détenus par le SCRS et cet article ne prévoit pas la divulgation à l'extérieur du gouvernement. Nous avons déjà

laissé entendre (rapport annuel de 1985-1986, page 55, rapport annuel de 1986-1987, pages 34-35) que l'on aurait peut-être intérêt à alerter les Canadiens membres d'organismes bénévoles qui subissent ou sont en danger de subir une influence étrangère clandestine. Il n'est pas du ressort du Service de décider quand il faudrait informer des membres du grand public au sujet de l'influence étrangère.

Cependant, il est inadmissible que les Canadiens accordent, en toute bonne foi, leur appui et leur participation à des activités de groupes de façade sous influence étrangère dont les desseins camouflés sont connus du SCRS. Il est également inadmissible que des organismes canadiens aux objectifs et aux méthodes légitimes deviennent, en toute bonne foi, la cible d'agents étrangers d'infiltration dont les buts véritables sont connus du SCRS.

Devrait-il y avoir des dispositions créant un organisme gouvernemental doté du pouvoir de décider quand le SCRS doit communiquer des renseignements de sécurité à des membres du grand public?

Le SCRS échange de l'information avec des organismes de police et de sécurité au Canada et à l'étranger. Nous avons appris que l'on prend soin de cacher des renseignements à certains pays où le régime en place pourrait s'en servir comme moyen d'oppression. Cependant, le SCRS ne possède aucun système de consignation des renseignements personnels défavorables qu'il communique à la police et à d'autres organismes. Cette situation nous semble incongrue, puisque l'article 38 de la *Loi* nous oblige explicitement à surveiller la communication de renseignements à d'autres organismes (voir page 6).

Devrait-on exiger explicitement du SCRS de tenir des dossiers statistiques de l'information communiquée aux organismes étrangers?

Menaces envers la sécurité du Canada

La pierre d'angle du mandat du SCRS se trouve dans la définition des menaces envers la sécurité du Canada, à l'article 2 de la *Loi*. Deux expressions dans cet article exigent des éclaircissements :

- *Influencé par l'étranger* : Dans son sens strict, cette expression est très claire; il ne fait aucun doute qu'une personne qui accepte en cachette de l'argent d'un gouvernement étranger pour faire adopter le point de vue de ce dernier par le public canadien s'adonne à une activité influencée par l'étranger d'une façon qui constitue une menace envers la sécurité du Canada. Mais la *Loi* ne tient certes pas compte du genre d'influence étrangère qui teinte les opinions et les discours de plusieurs, presque tous les Canadiens, — l'influence subtile de la publicité étrangère, de la littérature, de la télévision et des films étrangers, etc.
- *Préjudiciable aux intérêts du Canada* : Nous avons relevé une certaine imprécision dans la signification de cette expression qui revient dans l'étude de certaines plaintes. Est-il «préjudiciable aux intérêts du Canada» d'accomplir certaines choses (a) sans reconnaître publiquement qu'une personne (b) est à la solde d'une puissance étrangère. Ou existe-t-il une troisième condition particulière selon laquelle (c) il faut prouver qu'un dommage réel a été causé. Nous avons demandé un avis juridique indépendant au sujet de la signification de cette expression.

La Loi devrait-elle définir les expressions «influencé par l'étranger» et «préjudiciable aux intérêts du Canada»?

Le Solliciteur général a demandé au SCRS de n'employer que des techniques discrètes dans les enquêtes qu'il mène en vertu de l'alinéa 2d), visant des activités qualifiées globalement de «subversives». Toute enquête active au sujet de ces menaces exige maintenant l'autorisation personnelle du Solliciteur général. Nous avons applaudi à ces mesures de protection visant la défense d'une cause, la protestation et la manifestation d'un désaccord dans les règles de droit (voir chapitre 3). Mais la force de ces mesures n'a d'égal que l'engagement du Solliciteur général du jour. Ce que le Solliciteur général actuel peut ordonner, un autre, demain, peut le casser.

La Loi devrait-elle exiger des autorisations spéciales pour faire enquête sur des gens soupçonnés d'espionnage ou de terrorisme?

Habilitations de sécurité

L'article 42 de la *Loi* prévoit la révision (la nouvelle politique du gouvernement en matière de sécurité utilise le mot «redressement») lorsque l'administrateur général d'un ministère ou d'un organisme refuse un emploi fédéral à une personne ou lui fait perdre la possibilité de fournir des biens ou des services au gouvernement fédéral en raison d'une habilitation de sécurité refusée.

Mais il y a deux cas où une personne du secteur des affaires (publiques ou privées) n'a pas droit à une révision véritable lorsqu'une possibilité d'emploi lui a été refusée parce qu'elle n'a pas obtenu une habilitation de sécurité. La première, c'est lorsqu'elle se voit refuser un emploi ou est congédiée par un entrepreneur fédéral pour supprimer un obstacle à un contrat de vente au gouvernement fédéral.

Dans l'autre cas, aucun marché n'est en cause. Un exemple l'illustrera plus facilement. Dans les prochaines années, quiconque veut avoir accès aux locaux interdits d'un aéroport devra détenir une habilitation de sécurité assujettie à des vérifications pour lesquelles le SCRS joue un rôle primordial. Un pilote de ligne qui n'a pu obtenir d'habilitation ne pourra exercer son emploi. Cependant, aucun marché de fourniture de biens ou de services au gouvernement fédéral n'est en cause. Il s'agit plutôt de lignes aériennes qu'utilisent les services fédéraux. Cependant, la *Loi*, dans son libellé actuel, n'offre aux pilotes qui vivent pareille situation aucune possibilité véritable de révision en vertu de l'article 42. Les seuls recours possibles seraient une demande de révision départementale ou une demande aux Cours.

Nous pourrions étudier ces affaires en vertu de l'article 41 qui permet d'entendre les plaintes «contre des activités du Service», mais nous n'estimons pas qu'il s'agit d'une alternative convenable à une plainte formulée en vertu de l'article 42.

D'une part, l'article 41 ajoute une étape au processus en stipulant que la plainte doit d'abord être présentée au directeur du SCRS. Cette façon de procéder convient dans la plupart des cas. Ainsi, si le SCRS a commis une erreur par inadvertance, il doit pouvoir, disons, se rattraper. Mais une recommandation visant à refuser une habilitation de sécurité

est une décision que l'on suppose réfléchie et délibérée et que le directeur ne modifiera vraisemblablement pas.

Qui plus est, la *Loi* ne renferme aucune disposition explicite obligeant à communiquer au requérant toute information réunie en vertu de l'article 41. Cette situation, en général, s'explique. Dans les cas de plaintes formulées en vertu de l'article 41, c'est habituellement le plaignant qui accuse et le SCRS qui se défend. Les plaintes en matière d'habilitation de sécurité sont différentes. Ainsi qu'en traite le chapitre 7, nous avons l'obligation d'informer les auteurs d'une plainte en vertu de l'article 42, des soupçons qui pèsent contre eux afin qu'ils puissent répondre de façon éclairée aux questions de notre enquête. Il existe des dispositions semblables au chapitre de la communication dans les affaires de citoyenneté et d'immigration.

> *Un recours plus efficace s'impose-t-il dans le cas d'une personne privée d'un emploi dans une société privée parce que, sur l'avis du Service, une habilitation de sécurité lui a été refusée*?

La *Loi* prévoit, dans les cas de «refus d'une habilitation de sécurité» (article 42), un recours au moyen d'une plainte. Cependant, une interprétation trop stricte du mot *refus* pourrait créer un vide juridique puisque les autorités pourraient vraiment ne pas accorder une habilitation sans danger de plainte en laissant la demande dormir indéfiniment dans le panier des documents reçus, sans jamais la refuser catégoriquement. À notre avis, le mot «refus» devrait comprendre un délai «injustifié» tout comme une réponse explicite.

> *La Loi devrait-elle comprendre un délai injustifié dans sa définition du mot «refus»?*

Activités du SCRS

Nous avons déjà proposé (rapport annuel de 1986-1987, pages 14-15) que des dispositions visant des mandats d'urgence pourraient présenter une certaine valeur. L'obtention d'un mandat comporte actuellement 16 étapes. Une façon élaborée de procéder s'impose. Une des caractéristiques de la *Loi sur le SCRS* consiste à limiter l'emploi de pouvoirs d'intrusion; le SCRS ne devrait jamais pouvoir obtenir trop facilement un mandat.

Mais, tôt ou tard, une opération risque d'être compromise parce qu'on n'aura pas pu obtenir assez rapidement un mandat. Prenons le scénario où le SCRS apprend à la onzième heure qu'un terroriste fera un court arrêt au Canada. Un mandat instantané pourrait s'imposer afin de pouvoir surveiller électroniquement les réunions que tiendra le terroriste durant l'arrêt. C'est le genre de cas où la façon actuelle de procéder peut se révéler trop lourde. Nous continuons de tenir des statistiques sur le temps qu'il faut pour obtenir des mandats en suivant la façon normale de procéder.

Avec l'assentiment du Solliciteur général dans chaque cas, le directeur pourrait être autorisé à délivrer des mandats à court terme, non renouvelables, qui demeureraient en vigueur suffisamment longtemps pour permettre d'adresser une demande à la Cour fédérale : jusqu'à, disons, 96 heures. Nous envisagerions que tout mandat délivré d'urgence fasse l'objet, le plus tôt possible, d'un rapport à notre Comité.

Devrait-on autoriser le directeur, avec l'assentiment du Solliciteur général dans chaque cas, à délivrer des mandats à court terme dans des situations d'urgence?

Contrôle des mandats

Depuis que le Solliciteur général a annoncé le 30 novembre 1987 une «réorientation à mi-mandat», le Comité d'examen des demandes de mandat, constitué par le Service, comprend un «avocat du diable», un avoué qui relève du sous-solliciteur général du Canada et qui est chargé de contester toute demande de mandat. C'est là une parmi un certain nombre d'améliorations apportées à cette activité (voir chapitre 3).

À l'origine, cependant, nous avions proposé (rapport annuel de 1986-1987, page 12) que l'avocat contesterait devant le Solliciteur général (dans les cas où l'approbation personnelle s'impose avant que le SCRS puisse officiellement demander un mandat) ou devant la Cour fédérale (qui accorde ou refuse les mandats).

Après avoir davantage réfléchi à la question au cours de l'année écoulée, nous pensons maintenant que la Cour fédérale est l'endroit idéal pour cet avocat. Cette formule nous semble celle qui remplace le mieux le principe courant de justice naturelle : l'obligation d'entendre les deux parties d'un litige (*audi alteram partem)*. Dans les cas touchant à la sécurité, la cible ne peut manifestement pas être représentée directement devant le tribunal; cette façon de faire détruirait le but de, disons, l'écoute électronique, si la cible était prévenue grâce à la procédure en matière de mandat.

La Loi devrait-elle renfermer des dispositions visant la présence d'un avocat du diable aux auditions en vue d'un mandat et ce fonctionnaire devrait-il comparaître devant la Cour fédérale?

Le paragraphe 21(4)f) accorde explicitement aux juges de la Cour fédérale le libre arbitre d'inscrire des conditions dans les mandats. Dans la pratique, il semble y avoir certaines conditions particulières que les juges prennent en considération dans chaque cas. Elles visent ordinairement à protéger les communications privilégiées qui existent entre un avocat et son client, à savoir, par exemple :

- L'interdiction d'intercepter les communications à l'étude ou à la résidence d'un avocat ou à tout autre endroit dont il se sert habituellement pour recevoir des clients. (Il s'agit d'une protection semblable à celle que l'on trouve dans le *Code criminel* au sujet des mandats délivrés à la police.)
- Limite de l'interception des appels téléphoniques entre une cible et son avocat (ou un employé de l'avocat) à ceux que le directeur du SCRS ou un directeur général régional déclare liés à la menace envers la sécurité du Canada précisée dans le mandat.

Cette question a été traitée de façon assez détaillée dans notre rapport annuel de 1986-1987 (pages 22-23). La question que nous avions alors soulevée demeure donc toujours.

La Loi devrait-elle protéger de façon explicite, dans les enquêtes de renseignement de sécurité, les communications confidentielles entre un avocat et son client? Derrière cette question se cache une autre : *la Loi devrait-elle donner une*

liste des limites que les juges de la Cour fédérale peuvent imposer quand ils délivrent un mandat?

Contrôle

En vertu du paragraphe 39(3) de la *Loi*, les seuls renseignements que le SCRS peut nous refuser sont les renseignements confidentiels du Conseil privé. Comme nous l'avons déjà signalé, seule l'Australie possède un organisme indépendant à l'instar de notre Comité ayant un vaste accès aux dossiers de renseignement de sécurité. Dans notre travail quotidien, le secret frappant les renseignements confidentiels du Conseil privé ne nous a causé aucune difficulté.

Cependant, cette disposition limite manifestement la portée du contrôle que nous pouvons exercer. Nous n'avons aucun moyen de vérifier le rendement du Service face aux exigences du Cabinet. Nous n'avons aucun moyen de déterminer si les «difficultés» que nous avons relevées proviennent directement d'ordres émanant du Cabinet.

Ceux d'entre nous qui avons fait partie d'un Cabinet ne voyons aucune raison valable pour laquelle le Comité n'aurait pas accès aux décisions permanentes du Cabinet ou pour laquelle il y a insistance ou secret du Cabinet dans ce cas. Le principe du secret de Cabinet repose sur le besoin de permettre aux ministres d'exprimer leur désaccord dans la salle de réunion du Cabinet, puis de présenter un front uni une fois le débat terminé. C'est pourquoi le secret des débats du Cabinet et des documents sur lesquels ils portent est d'une importance cruciale à la solidarité ministérielle. Cependant, les décisions du Cabinet doivent être divulguées à ceux qui sont chargés de les mettre en oeuvre. Une fois prise, une décision est portée à la connaissance des fonctionnaires, mais pas à la nôtre.

Le Comité de surveillance des activités de renseignement de sécurité devrait-il pouvoir consulter les décisions prises par le Cabinet au sujet des activités du SCRS?

En règle générale, nous comptons sur les dossiers du SCRS pour obtenir des renseignements. Habituellement, cela suffit. Nous n'avons aucune raison de soupçonner le SCRS de tenter systématiquement de nous cacher des renseignements. Dans une société aussi libre que la nôtre, les secrets finissent toujours par s'éventer.

Cependant, des circonstances extraordinaires pourraient surgir où un membre du SCRS estimerait nécessaire de court-circuiter la filière pour dénoncer un travers qu'il a, estime-t-il, décelé dans le Service. Notre Comité serait l'endroit logique où ces dénonciateurs légitimes pourraient raconter leur histoire. Nous osons espérer que les dénonciateurs légitimes donneraient de préférence leurs histoires au Comité plutôt que de le dire à la Presse. Mais, la *Loi*, dans son libellé actuel, ne le protège pas contre toute mesure disciplinaire. Par contre, au Royaume-Uni, un fonctionnaire spécial a été nommé afin de recevoir les «fuites» des membres des services de sécurité («M1-5») et faire enquête. Les membres qui communiquent de l'information à ce fonctionnaire ne sont pas tenus de s'identifier.

La Loi devrait-elle au moins interdire les représailles contre un membre du Service qui communique de l'information au Comité?

Au chapitre 3 du présent rapport, nous avons abordé nos entretiens prolongés avec le SCRS au sujet de la publication de statistiques sur les mandats. Dans ce cas nous avons déterminés que:

> *Le Parlement devrait considérer si la Loi oblige la publication de statistiques sur des mandats précis.*

Accès à l'information et protection des renseignements personnels

Nous ne sommes pas sûrs que les rapports qui existent entre la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels*, d'une part, et la *Loi sur le SCRS*, d'autre part, n'ont pas encore été élaborés avec suffisamment de soin. Naturellement, le Comité est au courant du rapport du Parlement «Open and Shut» de mars 1987.

> *Le Parlement devrait-il modifier les lois afin de concilier les droits à l'accès à l'information et à la protection des renseignements personnels avec les nécessités de la sécurité nationale*?

Fondamentalement bonne

Après avoir examiné toutes ces questions, nous nous devons d'affirmer que nous considérons la *Loi* fondamentalement bonne. La plupart du temps et dans la plupart des cas, elle sert de cadre utile à la mise en application des cinq principes de base énoncés par la Commission McDonald :*

- La règle de droit doit être respectée.
- Le moyen d'enquête utilisé doit être proportionné à la gravité de la menace et à la probabilité de sa mise à exécution.
- Le besoin d'employer diverses techniques d'enquête doit être mis en regard du tort que cela pourrait causer aux libertés civiles, ou à des institutions sociales précieuses.
- Plus une technique comporte d'intrusion, plus l'autorisation d'y recourir doit venir de haut.
- Sauf dans les cas d'urgence, il faut utiliser les techniques de collecte de renseignements qui comportent le moins d'intrusion avant d'employer celles qui en comportent le plus.

Un organisme civil dont le mandat est énoncé dans une loi plutôt que dans un décret administratif, et qui est assujetti à un véritable contrôle politique et judiciaire et à un examen indépendant, demeure le genre d'organisme qui convient au renseignement de sécurité au Canada.

---

* *La liberté et la sécurité devant la loi*, Deuxième rapport de la Commission d'enquête sur certaines activités de la Gendarmerie royale du Canada (Ottawa, 1981), pages 539-540.

Annexe A

Directives ministérielles données au SCRS, 1987-1988

1. Dispositions en matière de consultations ministérielles.
2. Prérogatives ministérielles.
3. Divulgation de certains types d'informations.
4. Conduite d'activités impliquant certaines administrations étrangères.
5. Examen ministériel de dispositions administratives.
6. (Répétitions de directives ministérielles antérieures).
7. Instructions pour la gestion intérimaire.
8. Exécution de politiques gouvernementales.
9. Divulgation d'informations en matière d'autorité ministérielle.
10. Clarification de politiques ministérielles.
11. Divulgation d'informations aux autorités canadiennes.
12. Activités de vérification faites par le SCRS.
13. Conservation de renseignements.
14. Avis ministériel ayant trait aux questions administratives.
15. Conservation de certains types de renseignements et examen de questions opérationnelles.
16. Transfert du matériel du SCRS.
17. Délégation de l'autorité.
18. Mise au rebut des dossiers du SCRS.
19. (Répétition de directives ministérielles antérieures).

Annexe B

Résumé des plaintes en matière de sécurité examinées par le Comité de surveillance des activités de renseignement de sécurité, 1987-1988

Habilitations de sécurité

1. Activité subversive soupçonnée : une habilitation de sécurité a été refusée pour des motifs de malhonnêteté parce que la personne avait omis de fournir tous les renseignements au sujet de sa participation passée à une organisation considérée comme subversive par le SCRS, avait refusé de donner au SCRS les noms des autres personnes en cause dans cette organisation et, finalement, avait supposément falsifié des documents au sujet de ses études et de ses antécédents.

Au cours de l'enquête menée par le Comité, la personne a reconnu avoir commis une erreur grave de jugement quand elle a induit en erreur le SCRS au cours d'une entrevue au sujet de son degré de participation à l'organisation en cause. Elle a expliqué avoir «cédé à la panique». Elle a également avoué n'avoir pas répondu de façon totalement franche aux questions figurant dans la formule de demande d'emploi; l'information fournie était vraie, mais elle cachait la participation à l'organisation en cause. Le SCRS n'a fourni aucune preuve pour étayer ses soupçons de falsification de documents.

Les activités qui avaient éveillé les soupçons du SCRS au sujet de cette personne avaient pris fin cinq ans auparavant et cette dernière avait abandonné ses convictions de l'époque. Cette personne a commis des erreurs, mais ses explications étaient plausibles et son témoignage devant le Comité était franc et honnête.

Le SCRS et l'employeur ont également commis une erreur dans cette affaire. Le Comité a rejeté complètement l'idée selon laquelle le refus de donner les noms des autres membres avait sa place dans une recommandation du SCRS s'opposant à une habilitation de sécurité. L'employeur n'a pas, comme l'y oblige la politique du gouvernement en matière de sécurité, donné à la personne la chance de réfuter les soupçons du SCRS avant que l'habilitation soit refusée.

Le Comité a conclu qu'il serait peu probable que le plaignant se comporte de manière à présenter une menace envers la sécurité du Canada. Il a recommandé de lui accorder l'habilitation.

Citoyenneté

2. Terrorisme : la citoyenneté a été refusée à un immigrant reçu parce qu'on croyait qu'il s'adonnerait au genre d'activités définies au paragraphe 2c) de la *Loi sur le SCRS* comme une menace envers la sécurité du Canada, à savoir, «les activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage de la violence grave ou de menaces de violence contre des personnes ou des biens dans le but d'atteindre un objectif politique . . .dans un État étranger».

Le SCRS a déposé des preuves convaincantes selon lesquelles cette personne participait activement à une organisation terroriste. Elle a reconnu les délits criminels pour lesquels elle a été condamnée au Canada. Elle n'a pas contesté, par exemple, avoir aidé à charger

une cargaison illégale d'armes. Elle a tenté de convaincre le Comité qu'elle avait été mêlée à cette organisation sans savoir dans quoi elle s'embarquait. Mais ses propos vagues et ses pertes fréquentes de mémoire ont entaché sa crédibilité.

Le Comité a reconnu que le refus de la citoyenneté canadienne était justifié parce qu'il y avait des motifs valables de croire que cette personne demeurait une menace envers la sécurité.

3. Opposition retirée : La citoyenneté a été refusée à un immigrant reçu parce qu'il faisait partie d'une organisation jugée subversive par le SCRS. Suite à une modification apportée dans la façon de traiter les cas de subversion soupçonnée, annoncée par le Solliciteur général le 30 novembre 1987, et l'objection à ce que cette personne obtienne la citoyenneté a été retirée. Le Comité a donc clos le dossier. Cette personne est devenue depuis citoyenne canadienne.

4. Opposition retirée : Sauf qu'il s'agit d'une autre personne, cette affaire est semblable à la précédente dans ses moindres détails.

5. Opposition retirée: Dans le présent cas, le SCRS a retiré son opposition avant que le Comité n'entame son enquête; le dossier ne renferme donc aucune précision au sujet des soupçons.

Immigration

6. Criminalité : Une ordonnance d'expulsion a été rendue envers un immigrant reçu à la suite de rapports de renseignements criminels révélant qu'il faisait partie du crime organisé.

La GRC a déposé des preuves solides émanant de diverses sources et attestant de la participation du plaignant à des activités d'extorsion et de menaces pour le compte d'une organisation criminelle.

Le plaignant n'a pas témoigné en personne, même si on l'a invité à plusieurs reprises à se prévaloir de son droit d'être entendu. Dans un témoignage écrit, il a nié sa participation à toute activité criminelle organisée, mais n'a pas réfutée de façon convaincante tous les soupçons précis avancés par la GRC. Son avocat s'est limité à contester la compétence du Comité et à prétendre que la façon de procéder de ce dernier portait atteinte à la *Charte canadienne des droits et libertés*.

Le Comité a conclu que les formalités d'expulsion étaient justifiées.

7. Opposition retirée : L'entrée au Canada a été refusée à une personne parce que la GRC la soupçonnait de faire partie du crime organisé. Cependant, la Gendarmerie a retiré son opposition avant que le Comité n'entame son enquête; le dossier ne renferme donc aucune précision au sujet des soupçons.

Plaintes formulées en vertu de l'article 41*

8. Accusation de harcèlement : Une personne s'est plainte que le SCRS la soupçonnait sans raison d'avoir livré des secrets canadiens à un gouvernement étranger. De plus, elle s'est plainte que l'enquête menée par le SCRS avait nui à son bien-être physique et mental, ainsi qu'à sa réputation professionnelle.

On avait vu cette personne recevoir de l'argent d'un fonctionnaire étranger suspect. Le plaignant, aidé d'un avocat, a nié avoir trahi des secrets canadiens et a présenté des éléments de preuve afin d'étayer ses accusations selon lesquelles le Service se serait conduit de façon illégale et aurait fait preuve d'ingérence.

Le Comité a conlu que le SCRS était tenu de mener cette enquête et qu'il n'a pas utilisé ses pouvoirs de façon irraisonnable ou inutile.

9. Paiement d'une source : Une personne qui a fourni de l'information au SCRS s'est plainte de n'avoir pas reçu tout le montant convenu. La dispute a éclaté à la suite d'un malentendu. Après examen de la situation, le Comité a recommandé le règlement. Les deux parties ont accepté cette recommandation.

* En plus des affaires mentionnées dans le présent rapport, il y a eu 30 plaintes qui ne relevaient manifestement pas de la compétence du Comité ou dans lesquelles le plaignant se fondait sur aucun fait permettant de mener une enquête. Les plaintes décrites dans le présent chapitre sont celles pour lesquelles des enquêtes ont été menées et terminées.

Annexe C

Le réseau de renseignement au Canada

Le Service canadien du renseignement de sécurité (SCRS) fait partie d'un réseau d'organismes fédéraux qui s'occupent de la sécurité et du renseignement. La GRC mise à part, c'est l'organisme le mieux connu du grand public; c'est un élément essentiel; mais, néanmoins, ce n'est qu'un élément.

La présente annexe décrit les principaux éléments qui composent le réseau de renseignement. Elle résume un document qui, produit en 1987 à l'intention des membres du Comité de surveillance des activités de renseignement de sécurité afin de les aider dans leur étude du mandat du SCRS, situait cet organisme dans le contexte du travail effectué par d'autres organismes.* Le Comité a pensé que le public serait également intéressé. Nous avons dû faire de profondes coupures parce que une grande partie des renseignements contenus dans le document original sont secrets. En conséquence cette annexe est en aucune façon exhaustive. Toutefois, une grande partie de son contenu sera nouveau pour les non-initiés.

Sont décrits dans la présente annexe les postes et les organismes qui fixent les priorités et qui reçoivent, produisent, analysent et diffusent des renseignements; quand nous parlons de renseignements, nous voulons dire informations dans sa forme finale**, qui fournissent une base pour justifier l'action du gouvernement. La protection des biens (appelée ici «services de sécurité») y est abordée de façon accessoire. Nous tenons à souligner que la présente annexe est un document purement descriptif et qu'elle ne renferme aucune évaluation de postes ou d'organismes qui y sont nommés.

Le solliciteur général

Le solliciteur général est le personnage central du réseau de renseignement de sécurité, étant chargé non seulement du SCRS mais également de la GRC. Il est aidé dans son travail par le sous-solliciteur général, la Direction de la police et de la sécurité de son ministère et par l'Inspecteur général.

Le solliciteur général a, à l'égard du SCRS, un certain nombre de pouvoirs et de responsabilités aux termes de la *Loi sur le SCRS*. Il donne des directives écrites au SCRS sur la façon de traiter tant des affaires particulières que des catégories complètes de cas. Il doit approuver toute demande faite par le SCRS auprès de la Cour fédérale en vue d'obtenir un mandat pour employer certaines techniques d'intrusion telles que l'écoute téléphonique. Il doit également approuver toute entente intervenue entre le SCRS et un autre organisme, qu'il soit fédéral, provincial ou étranger.

---

* Le Comité tient à remercier de leur aide généreuse les nombreux fonctionnaires fédéraux qui lui ont fourni des renseignements sans obligation de leur part.

** Les analystes transforment les informations à la source en renseignements en évaluant leur fiabilité et en les interprétant pour déterminer leur signification. C'est le stade où il s'agit en même temps de traiter (c'est-à-dire traduire, interpréter des photos, répertorier) et d'analyser.

Un sigle vous intrigue . . . Le lexique vous l'explique

GEE — Le Groupe d'examen des évaluations; il s'agit d'un groupe d'étude qui revoit tout document rédigé par un GSEE avant qu'il soit déposé au CCR.

CCSR* — Le Comité du Cabinet chargé de la sécurité et des renseignements.

CST — Le Centre de la sécurité des télécommunications; il s'agit de l'organisme canadien chargé des renseignements sur les transmissions.

SCRS — Le Service canadien du renseignement de sécurité.

CRE — Le Comité de renseignements économiques, un rejeton du CCR.

CCR — Le Comité consultatif des renseignements; avec le CCS, c'est l'un des deux principaux comités du CISR; c'est un comité homologue du CRE.

CISR — Le Comité interministériel de la sécurité et des renseignements; il s'agit d'un comité formé de sous-ministres au service du CCSR; le CCS et le CCR constituent ses principaux sous-comités.

IG* — L'inspecteur général; il s'agit du haut fonctionnaire que le solliciteur général a chargé de surveiller le SCRS.

GSN — Le Groupe de la sécurité nationale; il s'agit de groupes de la GRC qui sont chargés, entre autres choses, d'assurer la liaison avec le SCRS et les autres corps policiers.

BCP — Le Bureau du Conseil privé; en sa qualité de secrétariat du Cabinet, c'est le centre nerveux des activités du gouvernement dans tous les secteurs, dont la sécurité et le renseignement.

GRC — La Gendarmerie royale du Canada; il s'agit du corps policier qui détient les responsabilités premières en matière de ...

CCS — Le Comité consultatif de la sécurité; il forme, avec le CCR, l'un des deux principaux sous-comités du CISR.

GSEE — Le Groupe spécial d'examen des évaluations; ces groupes constituent des groupes de travail auxquels le CCR commande des rapports sur les renseignements étrangers, ainsi que des documents de recherche plus longs sur des sujets particuliers.

CSARS — Le Comité de surveillance des activités de renseignement de sécurité; il s'agit de l'organisme qui, pour le compte du Parlement et du public, surveille le SCRS.

CARC — Le Comité d'approbation et de réévaluation des cibles; il s'agit d'un organisme interne du SCRS qui décide de l'objet et du degré de l'enquête.

Le sous-solliciteur général dispense aide et conseil au solliciteur général. Il coordonne l'élaboration de la politique et est souvent consulté par le directeur du SCRS. Sous l'autorité du sous-solliciteur général, la Direction de la police et de la sécurité entreprend, élabore et administre les politiques, les directives administratives et les systèmes de gestion pour le compte du solliciteur général. Cette Direction conseille également ce dernier sur les activités du SCRS, sur la GRC, les programmes fédéraux et nationaux d'exécution de la loi et d'antiterrorisme.

Service canadien de renseignement de sécurité (SCRS)

L'article 12 de la *Loi sur le SCRS* énonce le mandat général de cet organisme : «recueillir, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyser et conserver les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada, [...] de faire rapport au gouvernement du Canada et de le conseiller à cet égard».

Le Contre-espionnage et l'Antiterrorisme forment les deux grandes directions opérationnelles du SCRS. Une Direction de l'évaluation et de la production puise dans l'information fournie par les directions opérationnelles et auprès d'autres sources clandestines ou ouvertes pour produire du renseignement dont se serviront plusieurs services de l'État. Un autre programme important est celui des enquêtes de sécurité à l'égard des fonctionnaires et de toute autre personne qui ont accès à de l'information délicate ou à d'autres biens essentiels à la sécurité nationale.

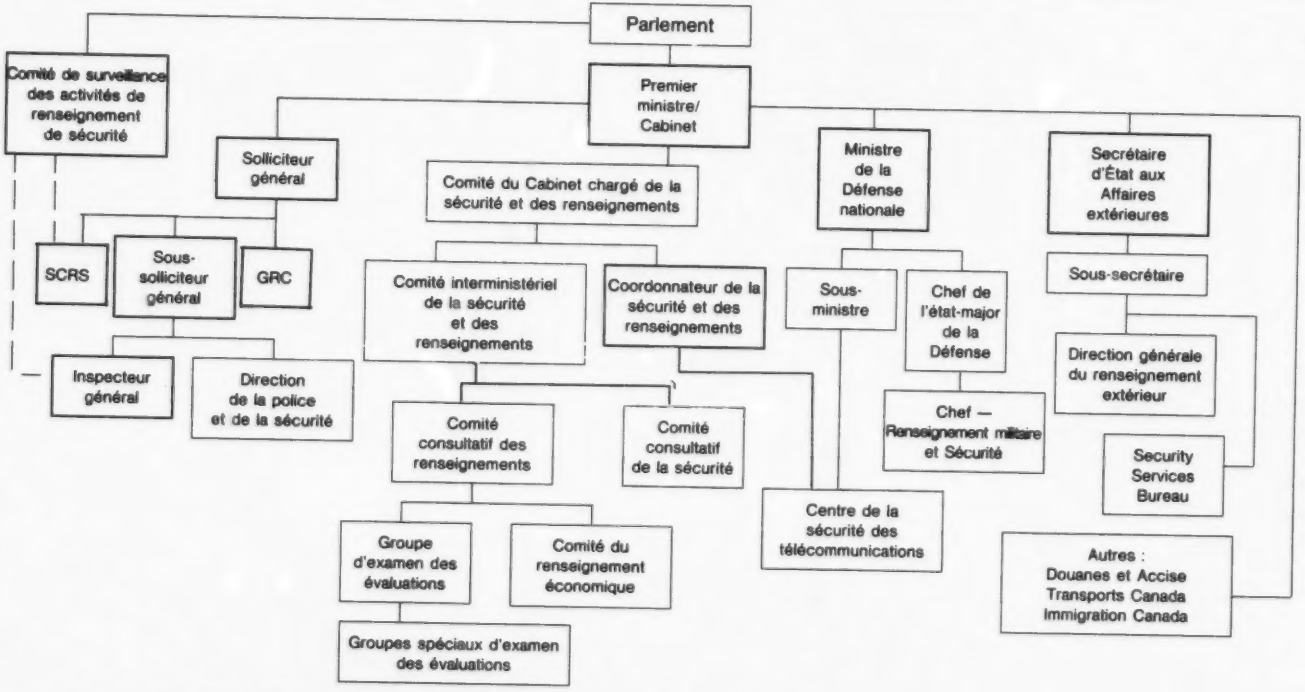
Le Comité Exécutif, le Comité de la politique opérationnelle et le Comité d'approbation et de réévaluation des cibles (CARC) jouent des rôles importants de coordination au sein du SCRS.

Étant donné que le travail du SCRS doit s'effectuer dans le secret, il fait l'objet d'un certain nombre de contrôles. Nous avons déjà traité du rôle du solliciteur général. Pour employer des techniques d'intrusion telles que l'écoute téléphonique, le SCRS doit obtenir des mandats de la Cour fédérale du Canada. La *Loi sur le SCRS* prévoit également la surveillance par deux cerbères externes : le Comité de surveillance des activités de renseignement de sécurité et l'Inspecteur général.

Inspecteur général

L'inspecteur général, qui relève du sous-solliciteur général, exerce, pour le compte du solliciteur général, la surveillance sur le SCRS, au chapitre de ses activités, de ses politiques, de ses lignes directrices et de ses contrôles internes. L'inspecteur général revoit le rapport annuel secret que le directeur du SCRS remet au solliciteur général et délivre un certificat attestant si a) il est satisfait dudit rapport, b) le Service a respecté les limites fixées par la *Loi* et par les directives du solliciteur général et c) le Service n'a pas utilisé ses pouvoirs de façon «abusive ou inutile».

À vol d'oiseau . . . principaux éléments du réseau de renseignement



Nota: a) Par souci de simplicité, nous n'avons indiqué que les liens les plus directs sur le plan de la hiérarchie.
b) Les boîtes noires indiquent les postes et les ministères occupant d'importantes responsabilités statutaires.

Comité de surveillance des activités de renseignement de sécurité (CSARS)

Le Comité exerce le droit de regard du Parlement et du public sur le SCRS. Il se compose de cinq membres nommés à temps partiel par le gouverneur en conseil après consultation du Premier ministre et des chefs des partis de l'opposition reconnus à la Chambre des communes.

Le double mandat que détient le Comité est énoncé dans la *Loi sur le SCRS* : le contrôle et les plaintes. En matière de contrôle, le Comité s'assure de l'efficacité du SCRS en accordant une attention toute particulière à ce que le Service n'utilise pas ses pouvoirs de façon «abusive ou inutile». Il fait également enquête au sujet des plaintes formulées à l'endroit du SCRS ou portant sur le refus d'habilitation de sécurité dans les cas d'emplois dans la Fonction publique, de marchés de l'État, d'immigration et de citoyenneté.

Le rapport annuel du Comité est déposé au Parlement et le public peut l'obtenir. Certains des rapports spéciaux que le Comité remet au solliciteur général sur des sujets particuliers sont également rendus publics.

Gendarmerie royale du Canada (GRC)

La partie IV de la *Loi sur le SCRS* (la *Loi sur les infractions en matière de sécurité*) confère à la GRC la responsabilité première d'arrêter les diplomates étrangers au Canada et les personnes qui menacent la sécurité du Canada. Le SCRS indique les menaces, mais c'est la GRC qui procède aux arrestations et réunit les preuves en vue des poursuites judiciaires. Dans l'exécution de cette responsabilité, la GRC oeuvre en étroite collaboration avec les autres corps policiers tant au Canada qu'à l'extérieur.

Au moyen de ses Groupes de la sécurité nationale (GSN), la GRC échange de l'information avec le SCRS et les autres corps policiers sur les crimes commis pour des motifs politiques, l'activité criminelle des extrémistes et toute autre question de sécurité nationale. Les Groupes ne font pas les enquêtes sur des délits particuliers mais réunissent, coordonnent et diffusent du renseignement criminel. Ils s'occupent également de diffuser des signalements de terroristes et d'évaluer les menaces que présentent des diplomates étrangers au Canada et des dignitaires étrangers qui visitent le Canada.

La GRC dispense également, aux aéroports et ailleurs, toute une gamme de services sécuritaires de consultation et d'autres genres de services en matière de protection aux hauts fonctionnaires de l'État, aux ambassades et aux consulats étrangers, et aux dignitaires qui visitent le Canada.

Transports Canada

La sécurité du réseau national de transport — sur terre, sur mer et dans les airs — et sa capacité de faire face aux situations d'urgence, en grande partie, relèvent de Transports Canada. L'accent sur la sécurité aux aéroports a pris de l'ampleur au cours des dernières années étant donné la fréquence des incidents terroristes dans les aérogares et à bord des avions dans plusieurs régions du globe.

Un directeur général, chargé de la Sécurité et de la Planification d'urgence, surveille le travail de quatre directions qui s'occupent a) de la politique et de la planification, b) des opérations de sécurité, c) du renseignement, de la sécurité des communications et du perfectionnement et d) de la planification d'urgence et du «coordonateur de contrôle des opérations» qui jouerait un rôle crucial advenant une situation d'urgence. Les directeurs régionaux de la sécurité relèvent également du directeur général.

La Direction des renseignements, de la sécurité des communications et du perfectionnement en sécurité a pour tâches, entre autres, a) de coordonner le rassemblement, l'analyse et la diffusion de renseignements émanant d'autres organismes et b) de rédiger des condensés de renseignements à l'appui des objectifs du Ministère, ainsi que c) d'évaluer les menaces contre la protection du réseau national de transport.

Emploi et Immigration Canada

Au chapitre du renseignement de sécurité, les intérêts d'Immigration Canada porte sur a) les tentatives déployées par les terroristes pour faire du Canada un refuge, une base d'activité ou un relais, b) les événements politiques et économiques qui surviennent à l'étranger et qui entraînent des mouvements migratoires internationaux pouvant faire entrer des immigrants légaux ou illégaux au Canada et c) les activités louches d'immigration, dont l'entrée illégale orchestrée de personnes au Canada, la production, la vente et l'utilisation de fausses pièces d'identité.

Une Division des renseignements produit deux genres de renseignements qu'elle qualifie de «stratégiques» et de «tactiques». Sur le plan tactique, elle élabore des programmes ou prend part à leur élaboration afin de déceler les pratiques frauduleuses en matière d'immigration, par exemple, elle distribue aux ports d'entrée des exemplaires de faux documents récemment découverts afin que les douaniers qui s'y trouvent sachent quoi chercher. Les renseignements stratégiques réunissent la documentation d'information, les études sur l'immigration et les analyses de tendances en matière d'activité d'exécution/de contrôle et la formulation de recommandations visant à améliorer les lois, les politiques et les méthodes.

Il y a également une Division du réexamen des cas et des catégories spéciales dont le travail, pour des motifs de sécurité, ne peut être décrit dans le présent rapport.

Immigration Canada envoie des avis de consultation au SCRS et aux autres organismes au sujet de toute demande de visa ou de résidence permanente au Canada afin de pouvoir déceler toute préoccupation de sécurité au sujet de la personne en cause.

Revenu Canada (Douanes et Accise)

Les préoccupations de Douanes et Accise en matière de renseignement de sécurité se présentent sous deux aspects : le «terrorisme et les stupéfiants» (le trafic de drogues pour financer des activités terroristes) et les exportations illégales de biens et de technologies de défense ou associés à la défense. C'est, à l'administration centrale, la Division de la répression de la contrebande et du renseignement et, à l'extérieur, les services de cette Division, qui s'occupent de ces domaines.

À l'administration centrale, la Division réunit les renseignements sur les dangers possibles, les méthodes et les voies de communication utilisées par les contrevenants et sur d'autres sujets qui feront l'objet de rapports de renseignement. Elle produit tant des renseignements tactiques destinés au service extérieur que des renseignements stratégiques à l'intention des cadres supérieurs en vue de la planification. Elle sert d'agent de liaison auprès des services douaniers des autres pays, des organismes d'exécution de la loi au Canada et d'autres organismes internationaux tels que le Conseil de coopération douanière et Interpol.

En vertu du Programme de contrôle des exportations qu'administre cette Division, les cargaisons destinées à l'exportation font l'objet d'une inspection afin de s'assurer que des biens et des techniques stratégiques ne sont pas exportés en infraction de la *Loi sur les licences d'exportation et d'importation.*

Ministère des Affaires extérieures

Le ministère est doté d'une Direction générale des services de sécurité qui est chargée d'élaborer et de formuler une politique visant la collaboration internationale contre le terrorisme, ainsi que la prestation d'une gamme de services de sécurité.

Au ministère des Affaires extérieures se trouve une Direction générale du renseignement extérieur qui réunit et analyse l'information qui servira à fournir du renseignement au Comité consultatif des renseignements (décrit ci-après) ainsi qu'au Ministère.

La Direction générale du renseignement extérieur comprend des divisions distinctes chargées du renseignement politique et du renseignement économique. L'affectation des analystes se fait selon la région (p. ex., le Moyen-Orient) ou des dossiers globaux (p. ex., la prolifération des armes nucléaires). Une troisième division interroge des immigrants choisis, des réfugiés politiques et des Canadiens qui ont vécu dans des sociétés fermées, afin de glaner de l'information utile qu'on ne peut obtenir des sources ouvertes. Ces entrevues n'ont lieu que sur consentement de la personne visée. La quatrième division assure le soutien administratif au reste de la Direction générale.

Ministère de la Défense nationale

Le chef, Renseignement militaire et Sécurité, est chargé de planifier et de diriger la collecte, la production et la diffusion du renseignement de défense, dont les renseignements scientifiques et techniques, nécessaire aux Forces canadiennes. Relèvent du chef un directeur général, Renseignement militaire, et un directeur général, Sécurité. Le directeur général, Sécurité, est chargé des services de sécurité du Ministère et des Forces armées.

Le Directeur général — Renseignement a la responsabilité de cinq directions : a) Renseignements de défense, b) Renseignement de situation, c) Exploitation photographique, d) Renseignement scientifique et technique, et e) Renseignement (Plans et doctrine). Le directeur général — Renseignement entretient également des rapports avec les organismes de renseignement des autres pays.

Centre de la sécurité des télécommunications (CST)

Le mandat du Centre est double : les renseignements sur les transmissions et la sécurité des télécommunications et des traitements des données assurés aux organismes fédéraux.

Le Centre fournit un service de renseignement sur les transmissions pour aider les politiques de défense et étrangère du Canada en captant les messages transmis par radios, radars et instruments électromagnétiques étrangers et distribue des rapports sur ce qu'ils révèlent. Il relève du ministre de la Défense nationale.

Le rôle du Centre en matière de services de sécurité de télécommunications consiste à aider les organismes fédéraux à empêcher les accès non autorisés à leurs télécommunications et au traitement d'information électronique. Le Centre fournit également aux ministères et organismes de la documentation et du matériel cryptographiques.

Comités de coordination

Il existe un certain nombre de liens directs, officiels et officieux, entre les divers organismes de sécurité et de renseignement. De plus, une série de comités a été constituée afin d'assurer la coordination.

Comité du Cabinet chargé de la sécurité et des renseignements

Ce Comité du Cabinet se trouve au coeur du réseau du renseignement de sécurité au Canada. Dirigé par le Premier ministre lui-même, il réunit des ministres dont les ministères a) font un usage important de renseignements étrangers et de sécurité, b) constituent d'importants générateurs ou producteurs de renseignements ou c) sont chargés d'activités de sécurité. Ce Comité établit la politique et fixe les priorités du gouvernement en matière de sécurité et de renseignement.

Bureau du Conseil privé (BCP)

Dans ce domaine, tout comme dans d'autres, le Premier ministre et le Cabinet reçoivent l'appui du BCP qui comprend un Secrétariat de la sécurité et du renseignement dirigé par le coordonnateur des Renseignements et de la Sécurité. Ce dernier est chargé a) de la coordination interministérielle et b) de l'information et des conseils dont le Premier ministre et le Comité du Cabinet ont besoin.

Comité interministériel de la sécurité et des renseignements (CISR)

C'est le greffier du Conseil privé qui dirige ce Comité réunissant les sous-ministres des ministères qui sont d'importants producteurs ou d'importants clients du renseignement (ou les deux), ainsi que le directeur du SCRS et le commissaire de la GRC.

Il a pour tâche d'élaborer des propositions destinées au Comité du Cabinet chargé de la sécurité et des renseignements. Il se compose de deux sous-comités principaux : le Comité consultatif de la sécurité (CCS) et le Comité consultatif des renseignements (CCR)

Comité consultatif de la sécurité (CCS)

Le CCS, au sein duquel siège le SCRS, s'occupe de questions de sécurité qui touchent les ministères fédéraux. Présidé par le sous-solliciteur général, il est appuyé par un secrétariat restreint.

Le Comité joue un rôle dans la formulation de la politique de sécurité avec une envergure interministérielle. Il conseille le CISR sur les exigences et les priorités en la matière. Il exécute certaines de ses fonctions par l'entremise de sous-comités chargés d'étudier des dossiers précis tels la protection de l'information et de la propriété, et l'antiterrorisme.

Comité consultatif des renseignements (CCR)

Le CCR constitue le haut lieu canadien du renseignement. À ce titre, ses membres coordonnent la production de renseignements, puisant aux travaux de recherche et d'analyse exécutés par des organismes fédéraux, notamment le SCRS, les Affaires extérieures, la Défense nationale et le Centre de la sécurité des télécommunications. Les analystes forment des groupes de travail appelés groupes spéciaux d'examen des évaluations (GSEE). Les documents produits par ces groupes sont revus par des groupes d'examen des évaluations (GEE) avant d'être remis au Comité pour qu'il les approuve et les diffuse.

C'est le coordonnateur de la sécurité et des renseignements du Bureau du Conseil privé qui préside le CCR. Le SCRS y est représenté par le directeur, de même que par un remplaçant désigné (niveau de sous-directeur).

Le Comité de renseignements économiques (CRE), important sous-comité du CCR, dirige la production de ce type de renseignements destinés au CCR. Le SCRS siège également au sein de ce sous-comité.

Enfin, le CCR conseille aussi le CISR sur des questions de principe comme les besoins en renseignements et la coordination des plans et programmes en la matière.

Annexe D

Personnel du Comité au 1er juillet 1988

Maurice Archdeacon, secrétaire exécutif	990-6839
Danielle Blache, secrétaire principale	990-8442
Annie Demirjian, adjointe exécutive	990-6319
Shirley Heafey, agent principal chargé des plaintes	993-4263
Arthur Graham, directeur de la recherche	990-8051
Maurice M. Klein, agent de recherche	990-8445
John M. Smith, agent de recherche	991-9111
Joan Keane, adjointe de recherche	990-8443
Madeleine DeCarufel, agent administratif et greffier	990-8052
John Caron, agent des dossiers	990-6838
Roger MacDow, commis des dossiers	998-5258
Diane Marion, secrétaire-réceptionniste	990-8441